VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Návrh a optimalizace počítačové sítě pro autodílnu

Design and Optimization of Information Technologies for a Car Workshop

Student: Jaroslav Beňa

Vedoucí bakalářské práce: Ing. Petr Rozehnal, Ph.D.

Ostrava 2018

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student: **Jaroslav Beňa**

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: 6209R017 Informatika v ekonomice

Téma: Návrh a optimalizace informačních technologií pro autodílnu

Design and Optimization of Information Technologies for a Car Workshop

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Úvod
2. Popis technologií a teoretických východisek
3. Analýza a popis současného stavu IT ve firmě
4. Návrh řešení a optimalizace IT
5. Výsledné zhodnocení navrženého IT řešení
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. aktualiz. vyd. Brno: Computer Press, 2013. ISBN 978-80-251-3176-3.

KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

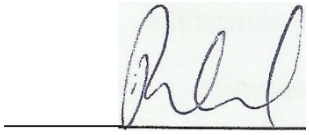
HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí: (praktické rady a návody) : podrobný průvodce začínajícího uživatele.* Praha: Grada, 2003. ISBN 80-247-0663-6.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

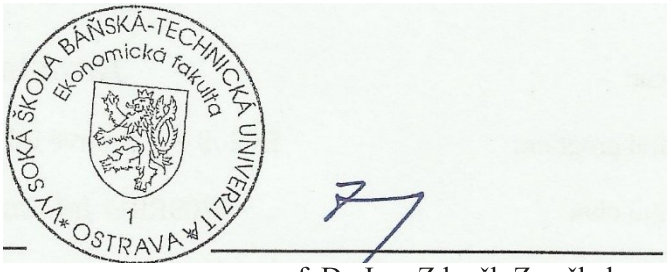
Vedoucí bakalářské práce: **Ing. Petr Rozehnal, Ph.D.**

Datum zadání: 24.11.2017

Datum odevzdání: 11.05.2018



Ing. Petr Rozehnal, Ph.D.
vedoucí katedry



prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

Chtěl bych vyjádřit poděkování vedoucímu bakalářské práce Ing. Petru Rozehnalovi, Ph.D. za odborné vedení a cenné rady při zpracování této bakalářské práce. Poděkování za morální podporu a trpělivost patří mé rodině, přátelům a mé přítelkyni.

Prohlašuji, že jsem celou práci vypracoval samostatně.

V Ostravě dne 9. 5. 2018

.....

Jaroslav Beňa

Obsah

1 Úvod

V současné době procházejí oblasti informačních technologií nevídanou evolucí pokroku počítačových a síťových technologií. Technologie počítačových sítí nám dnes poskytují stále rychlejší komponenty a média. Je to velký pokrok od dob malých, jednoduchých a pomalých sítí. Dnešní počítačové sítě jsou rozsáhlejší, komplikovanější, rychlejší a jsou součástí našeho každodenního života. S tím souvisejí i různé oblasti IT řešení, které využívají malé i velké firmy. V důsledku velkého rozmachu a integrace počítačových sítí, se stále více přesvědčujeme o tom, že počítač bez připojení k Internetu je sice dobrý pracovní stroj, avšak odříznutý od zbytku světa.

V této bakalářské práci bude cílem návrh a optimalizace IT s využitím moderních technologií s výhledem na stabilitu a bezpečnost informačních technologií a zhodnocení nově navrhnutého IT řešení dle požadavků firmy.

Tyto změny se firma rozhodla udělat z důvodu nespolehlivosti a špatné rychlosti počítačové sítě, která byla realizována pouze jedním Wi-Fi routerem s nedostačujícím dosahem pro interní prostředí autodílny. Dále chce firma vyřešit ukládání záznamů z IP kamer a zálohování dat na síťové úložiště včetně nastavení přístupových práv. Firma nikdy nedisponovala žádným zálohovacím síťovým úložištěm, přístupovými právy k datům u jednotlivých zaměstnanců a žádnými kamerami pro dohled nad zaměstnanci a firemním majetkem.

Ve druhé kapitole budou popsány technologie a teoretická východiska informačních technologií, které byly využívány v této bakalářské práci.

Třetí kapitola bude zaměřena na analýzu a popis současného stavu IT a prostředí firmy. Konkrétně zde bude stručně charakterizována firma, proběhne analýza prostředí, současného stavu sítě, a nakonec požadavky firmy na návrh nového IT řešení.

Ve čtvrté kapitole se zaměříme na návrh řešení a optimalizaci IT ve firmě. Bude navrhnut nový poskytovatel internetu, návrh firemní počítačové sítě včetně aktivních i pasivních hardwarových prvků, jejich rozmístění, zapojení a sestavení. Bude zde také návrh nových koncových zařízení, jejich konfigurace, nastavení zálohování a přístup k firemním datům pro jednotlivé osoby dle požadavků firmy.

Předposlední, pátá kapitola bude zaměřena na zhodnocení navrženého IT řešení. Bude zde otestováno a zhodnoceno IT řešení z funkčního i finančního hlediska. Finanční hledisko je důležité pro realizovatelnost tohoto projektu.

2 Popis technologií a teoretických východisek

V této kapitole budou popsána teoretická východiska, která byla podkladem pro řešení bakalářské práce. Požadavkům firmy mohou vyhovovat různé kombinace hardwaru, softwaru a nastavení sítě. Je třeba prostudovat každou eventualitu a vyloučit nepřípustné kombinace, nákladná řešení a řešení v dané lokalitě neuskutečnitelná.

2.1.Rozdělení počítačových sítí podle velikosti

Počítačové sítě se dělí podle různých specifických hledisek např. podle přepojování sítí a druhy přenášených signálů. Nás ale bude zajímat nejrozšířenější a nejznámější rozdělení, a to rozdělení podle rozlehlosti.

Existují taková rozdělení počítačových, kde jsou sítě seřazeny od nejrozsáhlejší po nejméně rozsáhlé:

- Sítě GAN – Global Area Network,
- Sítě WAN – Wide Area Network,
- Sítě MAN – Metropolitan Area Network,
- Sítě CAN – Campus Area Network,
- Sítě LAN – Local Area Network,
- Sítě PAN – Personal Area Network.

Pro potřeby bakalářské práce budou popsány dva typy počítačových sítí, a to WAN a LAN.

2.1.1. WAN

Wide Area Network (WAN) rozděluje datové, hlasové, obrazové a video informace na velké vzdálenosti jako město, země nebo stát. WAN není závislá na vlastním hardwaru pro přenos, ale může využít i veřejnou síť, pronajatou síť nebo soukromou komunikační síť. Sítě WAN tvoří řídící počítače, které jsou mezi sebou propojeny prostřednictvím komunikační podsítě. Jedná se nejčastěji o pevné telefonní linky nebo optické kabely, existují i družicová spojení. Vzájemné propojení mezi počítači probíhá zprostředkovaně – zpráva je předávána postupně od jednoho počítače ke druhému, a to až k cílovému místu (Bagad a Dhotre, 2009).

2.1.2. LAN

LAN (Local Area Network) je soukromá počítačová síť, která spojuje zařízení v kanceláři, budově nebo areálu v rozmezí několika kilometrů. LAN umožňuje sdílení zdrojů jako jsou hardware, software nebo data. Stanice, podporující síť LAN komunikují přímo pomocí běžného fyzického média, na bázi bod-bod bez jakéhokoli mezi přechodového přepínání. LAN se liší od ostatních typů sítí topologií, protokoly, přenosovými médii a velikostí sítě (Bagad a Dhotre, 2009).

2.2.Topologie počítačových sítí

Obsah této kapitoly se bude zabývat topologiemi počítačových sítí. Topologie je způsob, jakým jsou počítače v síti mezi sebou propojeny. Topologie je úzce spojena s kabeláží a určuje výsledné vlastnosti počítačové sítě.

Mezi základní topologie patří:

- Sběrnicová topologie,
- Kruhová topologie,
- Hvězdicová topologie,
- Stromová topologie.

Pro potřeby bakalářské práce bude popsána hvězdicová a stromová topologie počítačových sítí.

2.2.1. Hvězdicová topologie (Star Topology)

Každá stanice je připojena vlastním kabelem, nejčastěji kroucenou dvojlinkou. Kabely od stanic se pak soustředí do rozbočovače, který tvoří střed sítě. Pokud vznikne porucha jednoho kabelu, vypadne pouze jedna síť. Tato topologie je nejpoužívanější (Horák, Keršláger, 2011).

2.2.2. Stromová topologie (Tree Topology)

Stromová síť je vždy odvozena od nejvyšší neboli kořenové úrovně, ve které je jediný uzel, propojený s uzly druhé úrovně v hierarchii. Každý uzel druhé úrovně se pak propojuje s jedním nebo více uzly na třetí úrovni, z každé úrovně se tak vždy odvětvuje úroveň další. Musí existovat vždy alespoň tři úrovně, protože s pouhými dvěma úrovněmi bychom dostali topologii hvězdy. Pokud selže jeden uzel druhé úrovně, ostatní části sítě mohou dále pracovat (Sosinsky a Barrie, 2010).

2.3.Vrstvené modely

V této kapitole budou popsány vrstvené modely počítačové sítě, konkrétně sada protokolů TCP/IP a referenční model ISO/OSI.

2.3.1. Sada protokolů TCP/IP

Rodina protokolů TCP/IP rozeznává ve svém komunikačním modelu celkem čtyři vrstvy. V modelu TCP/IP známe pro formát přenosu a dat tři různé protokoly. Jsou to protokoly TCP a IP zmiňované výše a třetím protokolem je protokol UDP, který popisuje nespojovanou komunikaci. Protokoly TCP a UDP operují na transportní vrstvě, protokol IP je pak na úrovni síťové vrstvy (Sosinsky, 2010).

TCP/IP rozeznává ve svém komunikačním modelu celkem čtyři vrstvy:

- Aplikační vrstva,
- Transportní vrstva,
- Internetová vrstva,
- Vrstva síťového rozhraní.

Aplikační vrstva

Na aplikační vrstvě pracuje software, s nímž je v přímé interakci koncový uživatel. Mezi programy aplikační vrstvy patří webové prohlížeče, e-mailoví klienti, příkazové řádky, kancelářské balíky apod. (Sosinsky, 2010).

Transportní vrstva

Poskytuje transportní službu se zabezpečením přenosu uspořádaného proudu oktetů mezi komunikujícími aplikacemi protokolem TCP, resp. přenos datagramů mezi komunikujícími aplikacemi protokolem UDP (Burian, 2014).

Internetová vrstva

Zabezpečuje funkčnost na bázi 3. vrstvy v modelu OSI. Zajišťuje adresování sítě a nezabezpečenou výměnu paketů protokolem IP v síti, které jsou přenášeny přes mezilehlé prvky sítě (IP směrovače) (Burian, 2014).

Vrstva síťového rozhraní

Zajišťuje fyzickou komunikaci uzlů sítě, přičemž mapuje funkce fyzické a linkové vrstvy. Je to rozhraní sloužící pro přenos paketů protokolem IP různorodým přenosovým prostředím (Burian, 2014).

2.3.2. Referenční model ISO/OSI

Tento model rozděluje síťovou práci na vrstvy. Princip je v tom, že vyšší vrstva převezme úkol od nižší (podřízené) vrstvy, zpracuje jej a předá vrstvě nadřízené. Model je důležitý především pro výrobce síťových komponent (Horák, Keršláger, 2011).

Fyzická vrstva

Popisuje elektrické či optické, mechanické a funkční vlastnosti: jakým signálem je reprezentována logická jednička, jak přijímací stanice rozezná začátek bitu, jaký je tvar konektoru, k čemu je který vodič v kabelu použit atd. (Horák, Keršláger, 2011).

Aplikační vrstva

Je určitou aplikací, která zpřístupňuje uživatelům síťové služby. Zajišťuje přístup k souborům, vzdálený přístup k tiskárnám, správu sítě, elektronické zprávy atd. (Horák, Keršláger, 2011).

Prezenční vrstva

Má na starosti konverzi dat, přenášená data mohou být v různých sítích různě kódována. Tato vrstva zajišťuje sjednocení formy vzájemně přenášených údajů. V praxi často splývá s relační vrstvou (Horák, Keršláger, 2011).

Relační vrstva

Navazuje spojení mezi vzdálenými počítači a po skončení přenosu ukončuje spojení. Může provádět ověřování uživatelů, zabezpečení přístupu k zařízení atd. (Horák, Keršláger, 2011).

Transportní vrstva

Přenášené zprávy jsou děleny na pakety a opětovně se přijaté pakety skládají do zpráv. Při přenosu se mohou pakety ztratit nebo pomíchat (Horák, Keršláger, 2011).

Síťová vrstva

Vytváří spojení a směrování mezi dvěma počítači nebo celými sítěmi, mezi nimiž neexistuje přímé spojení. Zajišťuje volbu trasy při spojení. Volba trasy se nazývá směrování (routing) (Horák, Keršláger, 2011).

Linková vrstva

Přenáší údaje po fyzickém médiu, pracuje s fyzickými adresami síťových karet, odesílá a přijímá rámce, kontroluje cílové adresy každého přijatého rámce a určuje, zda bude rámec odevzdán vyšší vrstvě (Horák a Keršláger, 2011).

2.3.3. Základní protokoly

Protokol TCP

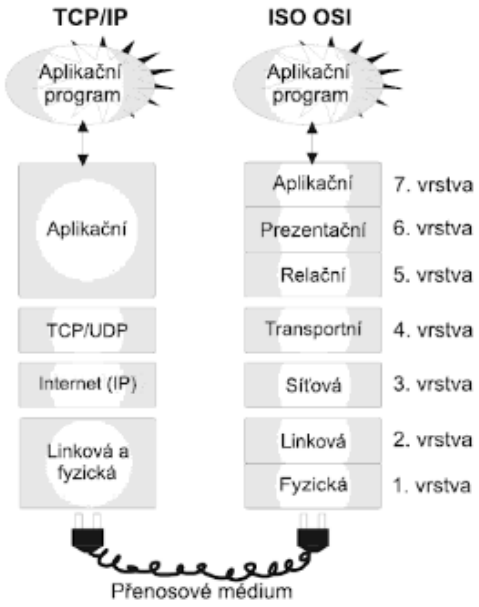
TCP protokol (Transmition Control Protocol) je jeden ze základní sady protokolů Internetu, typicky představuje transportní vrstvu komunikace. Použitím TCP protokolu mohou aplikace na počítačích zapojených do počítačové sítě vytvořit mezi sebou spojení, přes které lze přenášet data. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a e-mailový server) běžící na stejném počítači. TCP podporuje na internetu mnoho aplikačních protokolů a aplikací, včetně WWW, elektronické pošty a SSH (Secure Shell) (Procházka, 2010).

Protokol IP

IP protokol (Internet Protocol) je datový protokol, používaný pro přenos dat přes paketové sítě. Data se pomocí IP posílají sítí po blocích nazývaných datagramy (datový paket pro prostředí protokolu IP). IP protokol v doručování datagramů poskytuje nespolehlivou službu, označuje se také jako služba nejlepšího úsilí; tj. všechny stroje na trase se datagram snaží podle svých možností poslat blíže k cíli, ale nezaručují praktické doručení do cíle (Procházka, 2010).

2.3.4. Porovnání rodiny protokolů TCP/IP a ISO OSI

Soustavy síťových protokolů TCP/IP a ISO OSI se od sebe liší – jsou vzájemně neporovnatelné. Z obrázku 2.1. můžete vidět, že na síťové a linkové vrstvě jsou si velice blízké. Rodina síťových protokolů TCP/IP stejně neřeší linkovou a fyzickou vrstvu, proto se i na internetu setkáváme s linkovými a fyzickými protokoly z modelu ISO OSI.



Obrázek 2.1. - Porovnání TCP/IP a ISO OSI
Zdroj: Kabelová, 2012

2.4.IP adresa

IP adresa slouží k jedinečné identifikaci zařízení v rámci sítě. V současné době se k adresování využívá protokol IPv4 (Internet Protocol version 4), jenž definuje IP adresu jako 32 bitové číslo, psané dekadicky po jednotlivých oktetech (osmicích bitů), například 192.168.1.1. Teoreticky lze adresovat více, než 4 miliardy zařízení v rámci IPv4. Po vyčerpání tohoto limitu nastoupí IPv6 adresy. Ty jsou zapsány v hexadecimálním tvaru jako osm skupin po čtyřech číslicích oddělených dvojtečkami a využívají 128bitové IP adresy (Slavík, 2013).

Adresa IP se skládá ze dvou částí: net – ID (adresa sítě) a host – ID (adresa počítače). Podle toho, jak jsou jednotlivé sítě rozlehlé (kolik mají hostů) dělíme adresy do tří nejpoužívanějších tříd IP adres – A, B, a C. Třídy D se používá pro skupinové vysílání (multicasting) a třída E zůstala jako rezerva.

Třídy IP adres můžete vidět v tabulce 2.1.

	Rozsah adres prvního čísla	Počet čísel vyhrazených pro adresu sítě	Počet čísel vyhrazených pro adresu uzlu	Použití
Třída A	0–127	1 (adresuje 126 sítí)	3 (adresuje až 17 mil. uzlů = PC)	Rozsáhlé sítě
Třída B	128-191	2 (adresuje 16 tis. sítí)	2 (adresuje až 65 tis. uzlů)	Středně velké sítě
TřídaC	192-223	3 (adresuje 2 mil. sítí)	1 (adresuje až 254 uzlů)	Menší sítě
Třída D	224-239	multicast		
Třída E	240-255	vyhrazeno jak rezerva (výzkumné a experimentální účely)		

Tabulka 2.1. – třídy IP adres,
Zdroj: Horák a Keršláger, 2011 (vlastní zpracování)

Maska sítě

Maska sítě určuje, která část IP adresy patří adrese sítě a která náleží adrese hostitele. Hodnota masky sítě má také délku 32 bitů. Každý bit nastavený na hodnotu 1 přitom označuje část IP adresy vyhrazenou pro adresu sítě. Zbývající bity nastavené na hodnotu 0 znamenají adresu hostitele (Sanders, 2012).

2.5.Kabelová varianta

2.5.1. Ethernet

Prvně byl použit v 70. letech 20. stolení. Využívá se v LAN sítích a je definován pomocí standardu 802.2 a 802.3. V roce 1976 jej navrhla firma Xerox, poté se Ethernet postupně vyvíjel a dnes existuje více jeho variant.

V modelu ISO/OSI reprezentuje fyzickou a linkovou vrstvu a mezi jeho základní znaky patří kolizní přístupová metoda CSMA/CD. Díky rozšířenosti ethernetu existuje velké množství aktivních prvků. Při stavbě ethernetové sítě je nutné dodržovat topologická pravidla, především délku segmentů a celé sítě (Horák, Keršláger, 2011).

Prostřednictvím standardu 802.3 rozdělujeme Ethernet do několika variant. Níže budou popsány novější varianty Ethernetu.

Fast Ethernet (Ethernet pro rychlost 100 Mb/s)

Ethernet 100 Mb/s je nejrozšířenější nornou. Odpovídá doporučení IEEE 802.3. Jedná se o metodu přenosu dat, která je založena na přístupu CSMA/CD a ostatních pravidlech ethernetu. Na rozdíl od norem ethernetu pro rychlost 100 Mb/s není možné

použít koaxiální kabel. Kabely UTP musí být minimálně kategorie 5. Varianty Fast Ethernetu jsou 1000Base-TX, 100Base-FX a 100Base-T4 (Horák, Keršláger, 2011).

Gigabitový Ethernet (Ethernet pro rychlost 1 000 Mb/s)

Gigabitový Ethernet se někdy označuje 1000BaseX, kde písmeno X označuje konkrétní fyzickou vrstvu založenou na standardu ANSI X3.230 Fibre Channel. Topologie gigabitového Ethernetu je podobná rychlému Ethernetu (100BaseT). Všechny stanice se připojují k přepínači nebo rozbočovači a kolizní domény se důsledně kontrolují, aby správně fungovaly algoritmy pro detekci kolizí. Při použití UTP musí být kabel kategorie 5 a vyšší. Pracuje na Full-duplexním režimu. Varianty Gigabitového Ethernetu jsou 1 000Base-T, 1 000Base-TX, 1 000Base-SX a 1 000Base-LX (Trulove, 2009).

2.6.Bezdrátová varianta

Bezdrátové sítě neboli WLAN jsou stále nejoblíbenější nástroj pro rozšíření dosahu sítí na místa, kam se s klasickou kabeláží dostanete jen špatně anebo vůbec. Signál se přenáší elektromagnetickým vlněním, které nahrazuje metalické kabely. Elektromagnetické vlny se liší délkou a frekvencí. Bohužel volných frekvencí je málo, a tak na bezdrátové sítě zbyla nelicencovaná frekvence 2,4 GHz a frekvence 5 GHz. V pásmu 2,4 GHZ můžeme sítě provozovat bez obav, ale toto pásmo využívají i jiné technologie (mikrovlnné trouby, aj.), což způsobuje rušení přenosu. Provoz na pásmu 5 GHz je regulován pravidly Českého telekomunikačního úřadu (ČTÚ) (Horák, Keršláger, 2011).

2.6.1. Standardy síťového hardwaru

Jednotlivé síťové prvky je možno různě kombinovat. Můžeme používat určité topologie, přístupové metody a jiné kabely, kabeláž můžeme doplňovat o aktivní prvky atd. Tato variabilita může působit proti základnímu poslání sítí, různé sestavené sítě se spolu nemusí domluvit. Proto existují normy – standardy, které definují základní požadavky a technické provedení sítí. Organizace IEEE (Institute of Electrical and Electronics Engineers) provádí normalizaci standardů, tudíž jednotlivé normy nesou její označení. Nejpoužívanějším standardem tvořící bezdrátové sítě Wi-Fi je standard IEEE 802.11, který je popsán níže (Horák, Keršláger, 2011).

Standard 802.11

Tento standard vznikl v roce 1992 a definoval bezdrátovou síť v pásmu 2,4 GHz a rychlostech 1 nebo 2 Mbps. Postupem doby vznikaly v rámci této pracovní skupiny další pracovní podskupiny věnované rozšíření a změnám v tomto standardu. Poslední standard IEEE 802.11 byl publikován v roce 1999 a je zdarma dostupný. Standard 802.11 je nejpoužívanější technologií pro bezdrátové sítě Wi-Fi (Klement, 2017).

Přehled standardů IEEE 802.11 můžete vidět v tabulce 2.2.

IEEE 802.11	Datum vydání	Frekvenční pásmo v GHz	Šířka pásma v MHz	Rychlost v Mb/s
802.11-1997	Červen 1997	2,4	22	1, 2
802.11a	Září 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54
802.11b	Září 1999	2,4	22	1, 2, 5, 11
802.11g	Červen 2003	2,4	20	6, 9, 12, 18, 24, 36, 48, 54
802.11n	Říjen 2009	2,4 / 5	20/40	150
802.11ac	Prosinec 2013	5	20/40/80/160	886,7
802.11ad	Prosinec 2012	60	2160	6757

Tabulka 1.2. - Standardy IEEE 802.11
Zdroj: HomeToys, 2018 (vlastní zpracování)

Standard GSM

Globální systém pro mobilní komunikaci je nejrozšířenějším standardem pro mobilní telefony na světě. Telefon GSM vlastní asi polovina obyvatel planety Země z důvodu více SIM karet na jednoho člověka. GSM standard zavádí levnější datové přenosy pomocí paketových dat pod zkratkou GPRS.

2.6.2. Generace mobilních sítí

GPRS neboli General Packet Radio Service je mobilní datová síť, která je doplněná k síti GSM. Pro tuto technologii se také používá označení síť 2,5. generace (2,5G). GPRS nabízí rychlost 85 Kbit/s. V dnešní době se používá hlavně na e-maily nebo pro tzv. instant messaging.

EDGE je upravená verze GPRS a nabízí teoretickou rychlost až 238 Kbit/s. Ani EDGE se v dnešní době příliš nevyužívá.

Mobilní sítě 3. generace (3G sítě)

Do této generace patří UMTS systém s podporou kvality služeb (QoS) a rychlostí až 3,1 Mb/s.

Další generace je 3,5G (HSDPA), která spadá pod GSM a UMTS a dosahuje rychlosti až 14Mb/s.

Mobilní sítě 4. generace (4G sítě)

4G – je označení sítí čtvrté generace nebo LTE (Evolved UMTS Terrestrial Radio Access), jejichž cílem je dosáhnout rychlosti nad 100 Mbps při mobilním datovém přenosu. 4G sítě zvyšují sestupnou rychlostí řádově. Jsou navrhovány na využívání velmi rychlého webového přístupu, IP telefonie, na herní služby, Realtime Hight-Definition TV, přenos mobilního videa, videokonference a sledování 3D televize. U vyspělejšího 4G LTE+ je rychlost až 400 Mb/s v závislosti na typu telefonu a dostupných frekvencí (Jurášková, 2012).

2.6.3. Zabezpečení bezdrátových sítí

Existuje několik možností, jakým lze zabezpečit provoz bezdrátové sítě na straně klienta i přístupového bodu (Klement, 2017).

SSID

SSID představuje jméno sítě WLAN a stanice ho musí znát pro přístup k této síti, Ve skutečnosti představuje SSID velmi slabou formu zabezpečení. AP pravidelně vysílá rámec beacon obsahující toto SSID, a tak není problém běžnými přístroji toto SSID zjistit. U některých AP lze vypnout broadcast vysílání SSID (Klement, 2017).

Filtr MAC adres

Administrátor WLAN může pro AP vytvořit seznam MAC adres, které s ním mohou komunikovat. Tento přístup je ale značně nepraktický pro sítě větších rozměrů, a navíc je neúčinný díky tomu, že lze snadno změnit MAC adresu adaptéru. MAC adresu lze zjistit odposlechem komunikace a pomocí toho se útočník může přihlásit do sítě (Klement, 2017).

Protokol WEP

Protokol WEP (Wired Equivalent Privacy, tedy soukromí ekvivalentní s kabelovým přenosem) zajišťuje šifrování dat v rámcích 802.11 s pomocí symetrické šifry RC4. Pracuje se 40bitovými nebo 104 bitovými klíči a jedná se o algoritmus proudového šifrování dat v bezdrátovém spojení. Přítomnost šifry je indikována bitem WEP v poli FS (Field Control) záhlaví rámce 802.11. WEP se považuje za relativně slabou úroveň ochrany, protože jeho šifrovací mechanismus lze úspěšně napadnout.

Protokol WPA

Protokoly WPA (Wi-Fi Protected Access, chráněný přístup k Wi-Fi) a WPA2 jsou nejaktuálnější generací protokolů pro šifrování a autentizaci sítí 802.11x. Řeší některé problémy protokoly WEP tak, že zavádějí generování klíčů mechanismem TKIP (Temporary Key Integrity Protocol, protokol dočasné integrity klíčů). V rámci TKIP se používá 48bitový inicializační vektor IV a 128bitový šifrovací klíč, s jejichž pomocí je vygenerován nový klíč pro každý přenášený paket. Naproti tomu WEP používal stejný klíč pro všechny pakety. Pokud je v akci WPA, oba koncové body spojení mají stejný sdílený klíč (PSK, Pre-Shared Key). To znamená, že tento klíč nelze odečíst z komunikace, a WPA je proto mnohem bezpečnější.

WPA2 je úplnou implementací požadavků na bezpečnostní standard 802.11i. Všechna zařízení splňující normu pro WPA2 jsou povinně označena obchodní známkou s logem Wi-Fi. Součástí WPA2 je protokol CCMP (Cipher Block Chaining Message Authentication Code Protocol) a jeho opačný režim (Counter Mode). Využívá se přitom šifrovací algoritmus AES (Advanced Encryption Standard, pokročilý šifrovací standard) (Sosinsky, 2010).

2.7.Hardware sítě – aktivní prvky

V této kapitole budou popsány základní aktivní hardwarové prvky počítačové sítě, které jsou nezbytné pro její správné fungování. Pro potřeby bakalářské práce budou popsány prvky typu router, switch a Access point.

2.7.1. Router

Router (směrovač) je síťové zařízení, které vytvoří vnitřní síťové prostředí (domácí síť) a propojí jej s vnějším (Internet). Většina směrovačů disponuje několika porty určenými ke kabelovému propojení počítačů a také bezdrátovým rozhraním, přes které se připojují notebooky, chytré telefony či tablety. Směrovače operují na 3. vrstvě modelu OSI, kde odpovídají za předávání paketů mezi dvěma nebo více sítěmi (Horák, Keršláger, 2011).

2.7.2. Switch

Switch (přepínač) je síťové zařízení, obvykle bez možnosti konfigurace, které slouží ke kabelovému propojení počítačů. Na rozdíl od routeru musí veškerou síťovou logiku řešit jednotlivá připojená zařízení. Využívá se pro rozšíření počítačové sítě. Některé přepínače lze vzdáleně administrovat, jiné ne. Součástí administrovatelných přepínačů je obvykle agent SNMP (Simple Network Management Protocol), dále řádkové rozhraní CLI (Command Line Interface) na konzole a případně i webové rozhraní. Výhodou přepínače je, že nedochází ke ztrátě rychlosti sítě, protože počítače nejsou zahlcovány pakety. Výběr switche ovlivňuje například počet portů nebo možnost filtrování MAC adres. Přepínač podporuje plně duplexní režim, to znamená schopnost zasílat data přes více spojení zároveň ke stejnému počítači (Sosinsky, 2010).

2.7.3. Access point

Bezdrátový přístupový bod (AP) je zařízení kombinující vysílač a přijímač, a je zároveň uzlem bezdrátové sítě. Zařízení AP navíc dokáže propojit kabelovou síť s bezdrátovou. Jedná se o most mezi kabelovou a bezdrátovou sítí. Zařízení AP mohou podporovat standardy 802.11 a/b/g/n. Většina AP má DHCP, DNS server a funkci směrování. Dále existují tzv. dvoupásmová AP, která jsou schopna vysílat dvě sítě v reálném čase, což se hodí například do firmy pro vysílání firemní sítě a omezené sítě pro hosty, ušetří se tak na hardwaru a nutnosti pořízení dalšího AP (Sosinsky, 2010).

2.8.Hardware sítě – pasivní prvky

Tato kapitola bude popisovat pasivní prvky sítě, jako optické, metalické a koaxiální kabely a kroucenou dvojlinku. V této bakalářské práci budou detailněji popsány koaxiální kabel a kroucená dvojlinka.

2.8.1. Strukturovaná kabeláž

U strukturované kabeláže se vychází z různých standardů a celá síť je dělena na menší jednotky. Tyto jednotky se podle potřeby opakují a spojují do větších celků, ze kterých nakonec vznikne celá síť. Existuje několik standardů, které jsou vhodné pro implementaci síťových topologií, ale většina z nich se zaměřuje na obecnou, víceúčelovou a znovupoužitelnou síť, která bude vhodná pro cokoliv od hlasu po video. Standardy jsou navrženy pro správné fungování sítě na požadované rychlosti a popisují různé parametry pro testování sítě (Trulove, 2009).

Mezi strukturovanou kabeláž řadíme koaxiální kabel, optický kabel a kroucenou dvojlinku. Pro potřeby bakalářské práce bude detailněji popsána kroucená dvojlinka.

Kroucená dvojlinka

Je označována též jako TP (Twisted Pair). Data se přenáší rychlostí až 10 Gb/S na vzdálenost 100 m. Dva vodiče jsou vždy vzájemně kolem sebe obtočeny, čímž se minimalizuje EMI (Electromagnetic Interference) a ztráty způsobené kapacitním odporem. Jedná se o symetrické přenosové médium, signál je přenášen jako rozdíl napětí mezi těmito dvěma vodiči, což způsobuje menší náchylnost vedení k rušení a útlumu (Šilhavý, 2013).

Kroucená dvojlinka se vyrábí ve třech základních variantách. Níže jsou popsány dvě základní varianty kroucené dvojlinky.

UTP (Unshielded TP)

Jedná se o nestíněnou kroucenou dvojlinku, která se používá pro sítě typu LAN, případně pro telefonní systémy. Jednotlivé páry jsou zde uloženy ve vnější plastické izolaci. Maximální dosažitelná vzdálenost je okolo 100 metrů (Chromý, 2008).

STP (Screened TP)

Jedná se o stíněnou kroucenou dvojlinku, která má měděný plášť, opletený kolem kroucené dvojlinky nebo dvojlinek a poskytuje mnohem lepší ochranu dat než plášť nestíněné kroucené dvojlinky. STP má každý vodič krytý izolační fólií, navíc každý pár kroucených vodičů je také samostatně opláštěn. STP je tedy méně citlivá na elektrickou interferenci a podporuje vyšší přenosové rychlosti na delší vzdálenost než UTP. Typ ScTP – (Screened Twisted Pair) znamená, že je stíněn jen plášť kabelu a jedná se tak o částečně stíněnou kroucenou dvojlinku (Chromý, 2008).

2.8.2. Konektory

Konektory v této oblasti máme RJ-45 a RJ-11. Pro potřeby bakalářské práce bude detailněji popsán konektor RJ-45.

RJ-45

Nejrozšířenějším konektorem v oblasti počítačových sítí je RJ-45. Obsahuje 8 vývodů a používá se pro zapojení kabelů UTP a STP. Všech 8 vývodů využívá pouze při standardu 1 000Base-T.

2.9.Obecná definice Serveru

V technickém smyslu je server instancí počítačového programu, který přijímá a reaguje na požadavky jiného programu, známého jako klient. Méně formálně to může být každé zařízení, které spouští serverový software, považováno za server. Servery se používají ke správě síťových zdrojů.

Některé servery se zavázaly k určitému úkolu, často označovanému jako vyhrazené. V důsledku toho existuje řada vyhrazených kategorií serverů, jako jsou tiskové servery, souborové servery, síťové servery a databázové servery. Většina serverů je dnes sdílenými servery, které mohou v případě webového serveru převzít zodpovědnost s e-mailem, DNS, FTP, a dokonce s několika webovými stránkami.

Protože se běžně používají k poskytování nepřetržitě požadovaných služeb, většina serverů se nikdy nevypíná. V důsledku toho, selhání serverů může způsobit, že uživatelé sítě a společnost mají mnoho problémů. Servery jsou běžně prvotřídní počítače nastavené jako tolerantní k chybám (ComputerHope, 2017).

2.9.1. NAS server

Network Attached Storage (NAS) je souborově orientované řešení, které funguje jako tradiční souborové servery IT infrastruktury. Úložiště NAS jsou přístupné přes zmapované síťové ovladače, které komunikují se serverem a klientem přes síťový souborový systém nebo běžný internetový souborový systém prostřednictvím IP protokolu. Technologie serveru je jednoduchá pro webovou administraci a velmi spolehlivá. Do NAS se dají pořídit externí disky určité velikosti, které můžeme zapojit do diskového RAID pole. Takové zapojení má za následek nižší spotřebu a kompaktní velikost, což záleží na počtu disků. Síťové úložiště NAS poskytuje služby jako HTTP server, FTP server nebo Print server (ComputerHope, 2017).

2.9.2. RAID pole

RAID (Redundant Array of Independent Disks) odkazuje na sadu disků, které poskytují toleranci chyb u sdílených dat a aplikací. Skupina pevných disků se nazývá diskové pole. Disky, které pracují společně v konfiguraci RAID, se často označují jako jednotka RAID nebo pole RAID. V systému se více disků v jednotce RAID objeví jako jedna logická jednotka. Jednou z možností použití RAID je, že selhání jednoho disku nebude způsobovat katastrofické ztráty. Dalšími výhodami jsou zvýšená kapacita úložiště a potenciální sdílení více fyzických nebo logických pevných disků, aby se zajistila celistvost a dostupnost dat (Dean, 2009).

Typy RAID

RAID 0 a RAID 1

U RAID 0 se data ukládají střídavě na oba disky bez jejich dublování. U RAID 1 se data umísťují současně na oba disky. Dostupná kapacita disků u RAID 0 je součet kapacit obou disků. RAID 1 je maximální dostupná kapacita dána kapacitou nejmenšího v ní použitého disku.

RAID 1 se nejčastěji používá se dvěma disky. Data se na discích zrcadlí, což poskytuje toleranci při závadě jednoho disku.

RAID 5

Tento typ je velmi hodně používaný. K tomu, aby fungoval, je nutné mít zapojeny alespoň 3 disky. Z ukládaných dat se vytvoří redundantní kód, který slouží k opravě a znovuobnovení dat na zbylých discích, pokud dojde k poruše jednoho disku.

RAID 6

Je obdobou RAID 5 s tím rozdílem, že využívá dvě sady samoopravitelných kódů při ukládání jednoho souboru. Je odolný vůči současnému výpadku obou disků.

RAID 10

Používá se u stanic, které mají sudý počet disků. RAID nejprve spojí dva disky paralelně a vytvoří z nich jeden celek. Poté vezme zbývající dva disky a vytvoří z nich druhý celek. Tyto dva celky se pak zapojí do série RAID 1. Pokud selže jeden disk, tak je stále k dispozici druhý disk.

RAID 01

Obrácený RAID 10. Nejprve sečte kapacity obou disků do jedné větve a u čtyřdiskové stanice vytvoří druhou větev. Obě větve se spojí v RAID 1 paralelně (DigitálníDomácnost, 2014).

3 Analýza a popis současného stavu IT ve firmě

Kapitola se bude zabývat analýzou současného stavu IT ve firmě, a to včetně hardwarového, softwarového vybavení a internetového připojení, které firma v současnosti využívá.

3.1.Charakteristika společnosti

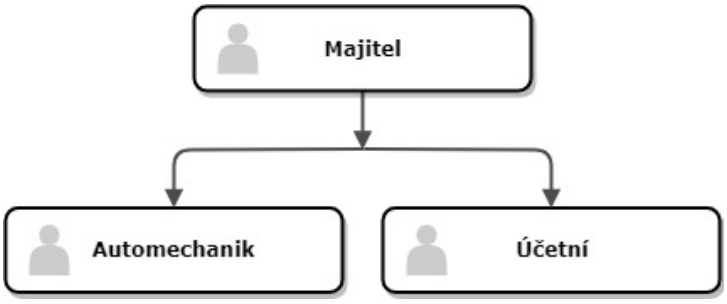
Společnost vznikla 27. 7. 2016 se v obci Blatnice pod svatým Antonínkem. V roce 2017 se kvůli velkému počtu zákazníků rozhodla rozšířit prostory své provozovny. Vznikl tedy velký sklad zboží odkupem starého domu určeného k prodeji. Společnost uzavřela smlouvy s velkými firmami jako Volkswagen, Škoda, Renault a BMW, jejichž dodávky dílů jsou kvůli velké poptávce přesouvány právě do tohoto skladu.

Hlavním předmětem podnikání společnosti jsou výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona a opravy silničních vozidel. Prodejem se rozumí prodej různého příslušenství jako jsou autolékárničky, hasící přístroje do automobilu, pneumatiky a další vybavení s auty související.

3.1.2. Organizační struktura

Majitel firmy je zároveň hlavní vedoucí oprav automobilů, který má pod sebou účetní a kancelář se dvěma pracovníky. Pracovníci jsou vyškolení automechanici a práci jim zadává buď majitel, nebo ji vykonávají sami spolu s majitelem společnosti. Osobní kontakt se zákazníky vykonává hlavně majitel a jeho dva zaměstnanci. Účetní společnosti pouze účtuje hotové zakázky a počítá výplaty zaměstnancům. Majitel se spolu s pracovníky bez problémů starají o sklad, přijímají objednané auto díly nebo je ze skladu používají. Ve společnosti všichni fungují tak, aby bylo dosaženo maximální optimalizace.

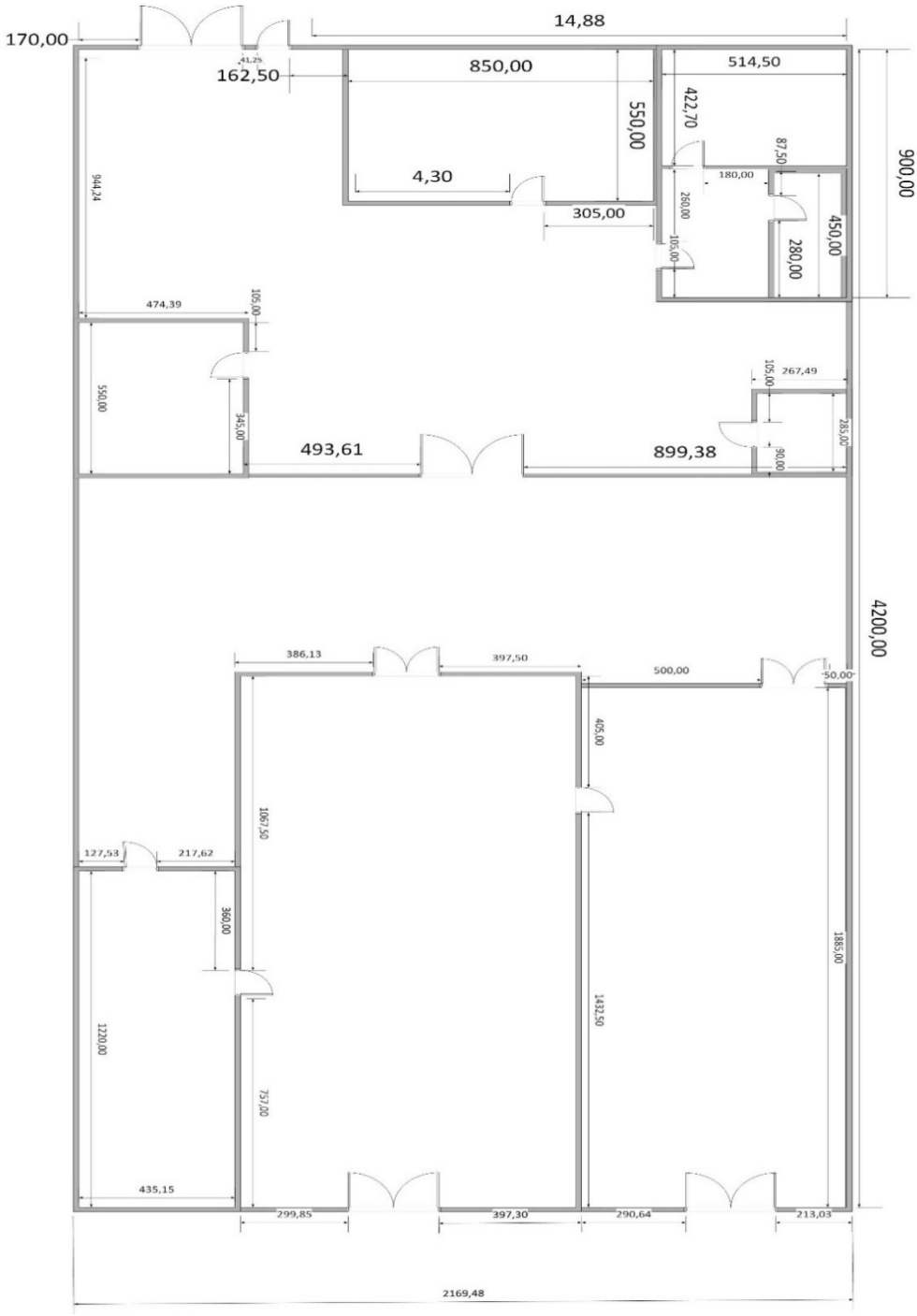
Organizační strukturu můžete vidět na obrázku 3.1.



Obrázek 3.1. - Organizační struktura
Zdroj: vlastní

3.2. Analýza prostředí

Provozovna se nachází v Blatnici pod svatým Antonínkem. Zde je postavena jednopodlažní budova s kancelářemi, sociálním zařízením, dílnou, skladovacím prostorem a místností pro zákazníky. Celková výměra činí 1321 m2. Pro návrh IT ve společnosti byl vypracován návrh půdorysu budovy včetně jednotlivých místností. Návrh můžete vidět na obrázku 3.2., kde jsou rozměry uvedeny v centimetrech.



Obrázek 3.2. – Půdorys budovy
Zdroj: vlastní

3.3. Analýza hardwaru a softwaru

Hardwarové i softwarové vybavení společnosti bylo zařízeno na velmi nízké úrovni. Po roce se společnost začala rozvíjet natolik, že stávající prostory, připojení k internetu a hardwarové i softwarové vybavení se stalo nedostačující. Vzhledem ke zvýšenému počtu zákazníků se společnost rozhodla kompletně modernizovat IT infrastrukturu a zvýšit tím spolehlivost a zabezpečení počítačové sítě a vzhledem k modernizaci zvýšit i bezpečnost instalováním zabezpečovacích kamer a síťovou zálohu dat. Na takovou modernizaci není momentálně IT ve společnosti stavěné, ať už dosahem Wi-Fi signálu pro prostory, které budou potřeba zasíťovat.

3.3.1. Současný stav IT ve společnosti

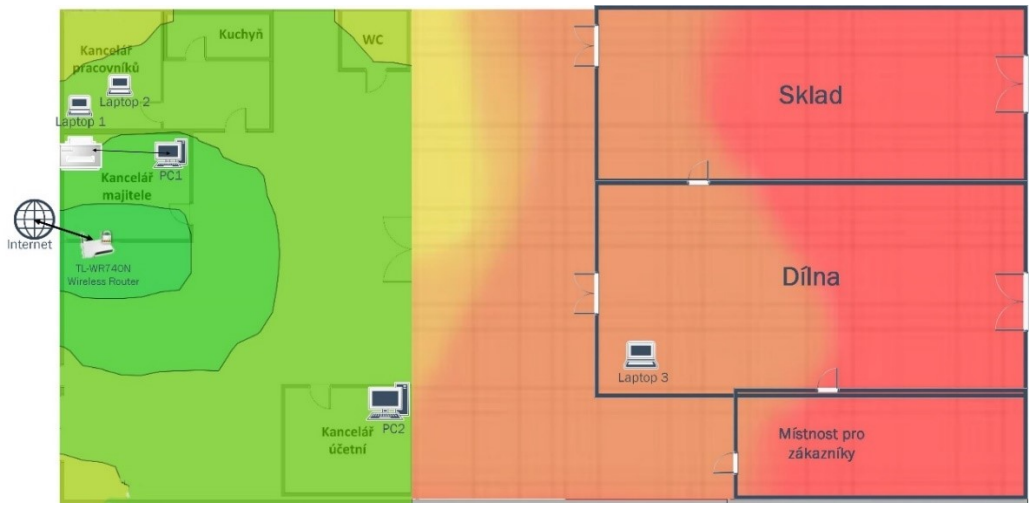
Centrální bod celé počítačové sítě je jediný Wi-Fi router, který je bohužel nejvíce vytíženým místem sítě. Připojení k internetu je realizováno pomocí tohoto routeru s automatickým přidělování IP adres a s technologií 802.11 g o maximální propustnosti 54 Mbit/s.

Síť má zabezpečení se šifrováním WEP, která je stejná pro majitele, účetní a zaměstnance. Nicméně letos se zjistilo, že zabezpečení WPA2 se dá lehce prolomit a útočník může takovou síť odposlouchávat. Každopádně by zabezpečení se šifrováním WPA2 bylo lepším řešením. Wi-Fi síť se potýká s méně častými výpadky a občas je potřeba restartovat router, aby fungovalo připojení k internetu. Dále se v kanceláři majitele nachází tiskárna, která je připojena pomocí USB kabelu k počítači a sdílena v rámci domácí skupiny, což je nevýhoda, protože je tiskárna závislá na zapnutém PC, ke kterému je připojena. Zálohování firemně důležitých a citlivých dat je řešeno prostřednictvím sdílené složky v počítači v kanceláři majitele. Účetní data jsou uložena v počítači účetní a jsou zpracovávány v účetním softwaru Money S3. Faktury, které jsou potřeba zaúčtovat ukládá majitel do svého počítače a jsou předávány prostřednictvím sdílené složky v rámci domácí skupiny. Takové řešení má za následek malou bezpečnost dat, protože se k těmto datům dostane každý, kdo je připojen k síti, přičemž s přístupem do této složky nejsou spjata žádná přístupová práva, určená jednotlivým zaměstnancům a musí být vždy zapnutý počítač v kanceláři majitele, aby byla data přístupná.

Wi-Fi router má výchozí bránu 192.168.0.1 a přidělování IP adres zajišťuje automaticky nastavený DHCP server v rozsahu 192.168.0.1 - 192.168.0.199 bez podsítí.

Poskytovatel internetu je nespolehlivý z toho důvodu, že začínající firma volila nejlevnějšího poskytovatele internetu v okolí, kvůli snadnému a rychlému příjezdu technika.

Následující obrázek 3.3. ukazuje rozmístěný hardwarových prvků a pokrytí stávajícího Wi-Fi signálu.

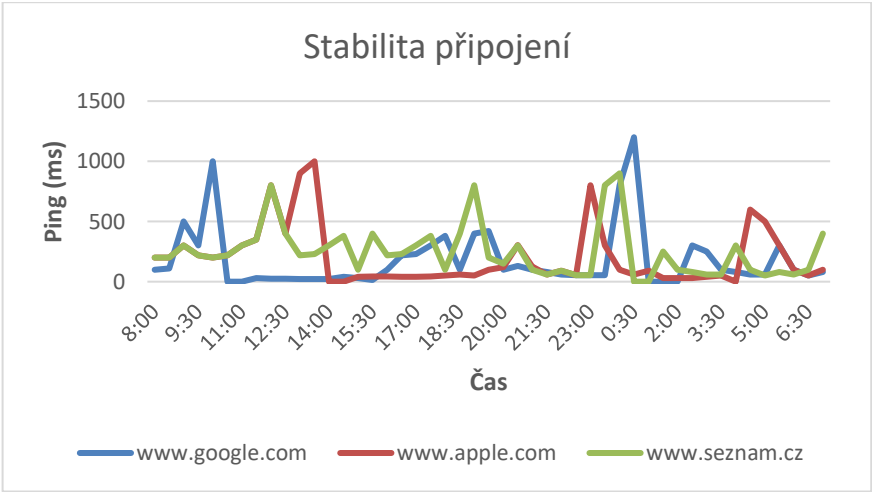


Obrázek 3.3. – Teplotní mapa bezdrátové sítě
Zdroj: vlastní

Připojení k internetu

Současný poskytovatel internetového připojení (ISP) Blanet, s. r. o. poskytuje v dané vesnici připojení k internetu 10/2 Mbit/s. Toto připojení trpí výpadky internetu a v rámci modernizace IT pro zálohování firemních dat a vzdáleného přístupu k serveru musí být vybrán jiný ISP. Internet musí být stabilnější, rychlejší a nesmí mít takovou míru náchylnosti na meteorologické vlivy.

Současnou spolehlivost připojení můžete vidět v grafu 3.1.



Graf 3.1. – Současná spolehlivost počítačové sítě
Zdroj: vlastní

3.4.Požadavky Firmy

Po analýze a následné konzultaci s majitelem si firma určila tyto požadavky pro modernizaci své IT infrastruktury:

- Rozšíření signálu Wi-Fi do zbytku firmy,
- Výběr spolehlivějšího a stabilnějšího internetového připojení,
- Vyšší zabezpečení lokální sítě LAN a WLAN,
- Řešení pro zálohu a manipulaci s firemními daty důležitých a citlivých firemních dat,
- Možnost přístupu k firemním datům mimo prostředí firmy,
- Bezpečnost dat a nastavení určitých oprávnění,
- Instalaci zabezpečovacích kamer a ukládání záznamů na server po určitou dobu,
- Připravenost sítě pro další rozšiřování,
- Rozpočet v rozmezí 20000–40000 Kč.

4 Návrh řešení a optimalizace IT

Tato část práce bude zaměřena na vlastní návrh síťové infrastruktury ve firmě. V návrhu se bude vycházet z teoretických poznatků a analýzy současného stavu tak, aby bylo dosaženo stanovených cílů a požadavků firmy. Bude zde navržen nový poskytovatel internetu, výběr aktivních a pasivních prvků, včetně jejich umístění. Dále zde bude popsána konfigurace jednotlivých prvků sítě, včetně koncových zařízení. V poslední řadě budou nastavena přístupová práva a vytvoření adresářové struktury.

4.1.Návrh počítačové sítě

Počítačovou síť je vhodné realizovat podle standardu IEEE 802.11n. Ve prospěch tohoto standardu je hlavně dosažení vyšších přenosových rychlostí v okolí firmy, kde existuje minimum obsazených kanálů pro pásmo 2,4Ghz a z toho důvodu tuto síť budou minimálně rušit okolní bezdrátové sítě. Pásmo 2,4Ghz jsem vybral z důvodu lepšího dosahu signálu, než má pásmo 5Ghz. Splnění požadavků na pokrytí je jedním z hlavních prvků právě při jejím plánování. Řešením může být návrh orientační mapy, spolu s nákresem rozmístění přístupových bodů a oblastmi jejich dosahu, resp. pokrytí. Od Wi-Fi sítí se často požaduje mobilita. Z tohoto důvodu je třeba zajistit plynulý přechod od jednoho přístupového bodu k jinému. Dalším důležitým parametrem návrhu je počet uživatelů a jejich nároky na tuto bezdrátovou síť (rychlost, odezva, kvalita signálu). Následně se navrhne i vhodný princip přidělování IP adres a v neposlední řadě způsob zabezpečení sítě.

4.1.1. Výběr hardwarových prvků

Vzhledem k rozhodnutí realizovat vznikající bezdrátovou síť podle standardu IEEE 802.11n je třeba zajistit HW zařízení, které již s tímto standardem pracují.

Byl vybrán VDSL Wi-Fi router ASUS DSL-AC55U, který podporuje standardy 802.11b/g/n/ac na pásmech 2,4 GHz a 5GHz. Obsahuje 5x port RJ-45, 1x port WAN, 1x port RJ-11 a pro případné budoucí rozšíření disponuje technologií VDSL2 a záložním 3G/4G modemem pro vložení SIM karty. Samozřejmě nechybí jednoduché řízení kvality služeb (QoS), silné možnosti zabezpečení s podporou WPS, možnost vytváření oddělených sítí pro hosty, podpora DLNA sítí, VPN server, SPI firewall, ochrana proti DoS útokům, kontrola přístupu, rodičovská kontrola, Network service filtr, URL filtr nebo Port filtr.

K připojení jednotlivých prvků sítě budou využita zařízení typu switch a pro samotné rozšíření sítě do zbytku prostor budou sloužit dvě dvouportové zásuvky RJ-45 a jeden Access point typu Dual-Band. Byly vybrány následující:

- 2x 8 portový switch TP-LINK TL-SG108 s rezervou pro budoucí rozšíření,
- 2x zásuvky pod omítku Datacom RJ-45 CAT6 STP, 2x RJ45,
- 1x přístupový bod (Access Point) TP-LINK RE305 AC1200 Dual Band.

Přístupový bod bude vysílat dvě sítě, z nichž jedna bude na pásmu 2,4Ghz pro pokrytí zbytku prostoru ve firmě Wi-Fi signálem a druhá na pásmu 2,4Ghz bude vyhrazena pro hosty.

Zásuvky RJ-45 budou propojeny kabelem určeným pro rozvody strukturované kabeláže UTP CAT.6 ve verzi drát vedené ve zdi. Ostatní prvky budou propojeny kabelem UTP CAT.6 typu LAN, který je zakončen konektory RJ-45. Tato verze UTP byla vybrána z důvodu rychlosti, propustnosti a spolehlivosti a tyto parametry jsou více než dostačující pro potřeby firmy.

Veškerý hardware byl vybrán na základě analýzy navrhované sítě, kterou majitel požaduje a všechny aktivní i pasivní prvky byly cenově prokonzultovány a schváleny. Veškeré aktivní i pasivní prvky byly vybrány pro potřeby nové počítačové sítě a jsou pro síť ideální.

4.2.Návrh nového poskytovatele internetu

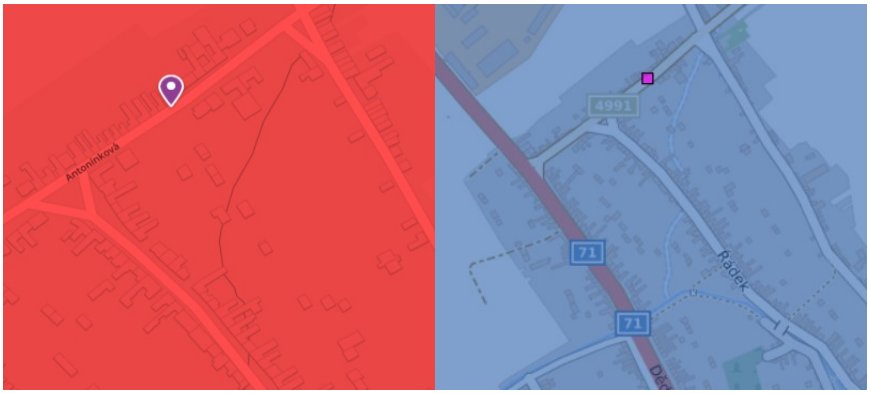
Na základě analýz původní počítačové sítě a následného návrhu bylo rozhodnuto, že bude změněn poskytovatel internetu z důvodu špatné stability a rychlosti původní počítačové sítě, která byla nedostačující pro potřeby firmy a nově navržený síťový hardware.

V Blatnici pod svatým Antonínkem působí hned několik poskytovatelů internetu, z nichž jsem vybral společnost Dat, s. r. o., která poskytuje telekomunikační služby od roku 2002. Bude využita technologie VDSL, která nabízí znatelně vyšší rychlosti připojení k internetu a také zásadně vyšší rychlost pro odesílání dat (nahrávání dat na internet), a to za stejnou cenu, za jakou je stále nabízeno ADSL. Maximální teoretická propustnost pro danou oblast bude tedy 65/34 Mbit/s (Dat, 2018).

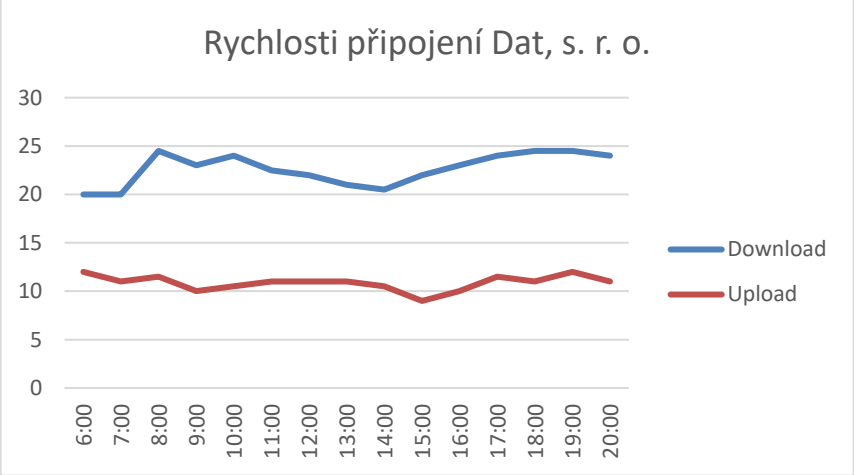
Implementace tohoto připojení je jednoduchá, levná a má minimální měsíční náklady. Pro potřeby připojení k internetu mimo firmu, kvůli výjezdům mechaniků, bude zřízeno mobilní připojení ve formě USB disků od operátora Vodafone Czech Republic, a. s., s maximální teoretickou rychlostí 178/56 Mbit/s.

Firma bude využívat připojení 4G/LTE s frekvencí 800MHz, kterou společnost Vodafone Czech Republic, a. s. podporuje.

Dostupnost pro cílovou oblast byla ověřena přímo na webových stránkách firmy Vodafone Czech Republic, a. s. a webu Českého telekomunikačního úřadu pro pásmo LTE 800 Mzh (Obrázek 4.1.). Připojení od firmy Dat, s. r. o., bylo testováno v průběhu celého pracovního dne a naměřené reálné rychlosti můžete vidět v grafu 4.1.



Obrázek 4.1. – Mapa pokrytí 4G LTE 800 Mhz, z leva Vodafone, Český telekomunikační úřad, Zdroj: Vodafone Czech Republic, a. s., 2018; Český telekomunikační úřad, 2018 (vlastní zpracování)

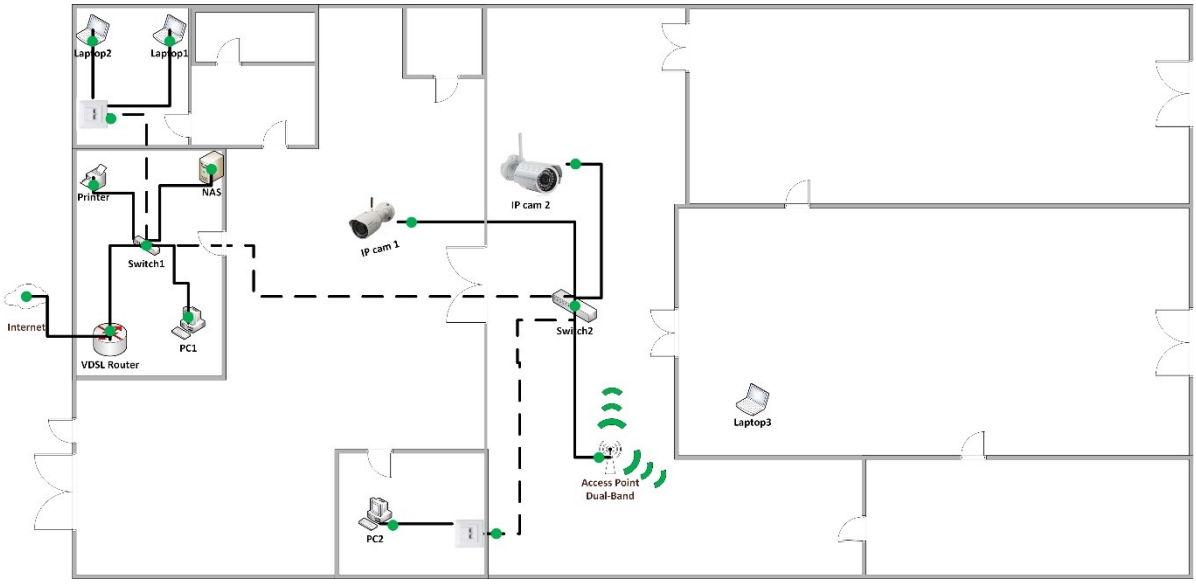


Graf 4.1. – Rychlosti download a upload nového internetového připojení, Zdroj: vlastní

4.2.1. Fyzická topologie sítě

Vzhledem k rozmístění hardwarových prvků počítačové sítě bude zvolena topologie typu hvězda. Tato topologie je výhodná. Pokud selže jeden počítač nebo kabel, který ho připojuje k rozbočovači, pouze ten nefunkční počítač nebude moci posílat nebo přijímat data ze sítě. Zbývající část sítě bude fungovat normálně. Hlavní prvkem bude VDSL Wi-Fi router, ze kterého povede UTP kabel do každé místnosti, a to většinou do switche nebo zásuvky ve zdi. Ze switche nebo zásuvky pak povede UTP kabel do koncových zařízení jako jsou počítače, notebooky, tiskárna, Access Point, NAS a IP kamery.

Rozmístění HW prvků můžete vidět na obrázku 4.2.



Obrázek 4.2. – Fyzická topologie sítě,
Zdroj: vlastní

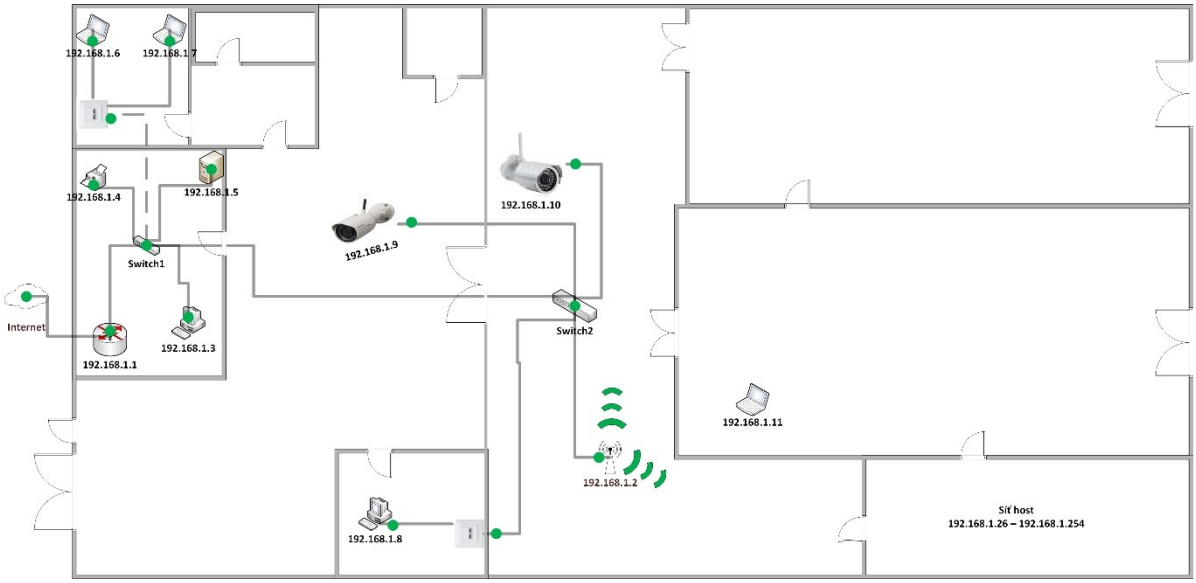
4.2.2. Logická topologie sítě

Pro strukturu počítačové sítě bude použita IP adresa třídy C a to 192.168.1.0 s maskou 255.255.255.0. Rozsah IP adres je v rozmezí 192.168.1.1 až 192.168.1.254 a pro takové rozdělní je přidělena IP adresa broadcastu 192.168.1.255. Pro VDSL Wi-Fi router bude přidělena adresa 192.168.1.1. Dalším hlavním prvkem je Access Point, který bude mít IP adresu 192.168.1.2.

Následující rozdělení IP adres se týká zařízení, které budou připojeny k hlavním prvkům. To se týká zařízení, které jsou majetkem firmy a jsou připojeny pomocí UTP kabelu k síťovému prvku. Rozdělení IP adres bude tedy následující: Počítač v kanceláří majitele bude mít IP adresu 192.168.1.3, síťová tiskárna 192.168.1.4, síťové úložiště NAS 192.168.1.5, počítače v kanceláři pracovníků budou mít rozsah 192.168.1.6 až 192.168.1.7, počítač v kanceláři účetní 192.168.1.8 a v poslední řadě IP kamery 192.168.1.9 až 192.168.1.10. Notebook majitele, který je umístěný v dílně, bude připojen do firemní sítě pomocí Wi-Fi a bude mít IP adresu 192.168.1.11. Musí se počítat s tím, že budou do firemní sítě v budoucnu napojená i jiná zařízení. Pro tento případ bude vyhrazen rozsah IP adres od 192.168.1.12 až 192.168.1.25 včetně rezerv. Tím se myslí připojení dalších počítačů, tiskáren a notebooků. Taková zařízení budou v síti pak snadno identifikovatelná.

Pro zařízení, která se budou připojovat přes Wi-Fi pro hosty, jakou jsou mobilní telefony a notebooky, které potřebují pouze přístup k internetu, bude vymezen rozsah IP adres od 192.168.1.26 – 192.168.1.254 přidělovány automaticky DHCP serverem a taková zařízení nebudou mít přístup do firemní sítě.

Logickou podobu sítě můžete vidět na obrázku 4.3.



Obrázek 4.3. - Logická topologie sítě,
Zdroj: vlastní

4.3.Nastavení aktivních prvků sítě

Tato podkapitola bude zaměřena na nastavení aktivních prvků počítačové sítě, jako jsou VDSL Wi-Fi router, switch a Access Point, včetně jejich zabezpečení.

4.3.1. Konfigurace VDSL Wi-Fi routeru

Nastavení routeru se provádí prostřednictvím webové administrace tak, že do adresního řádku internetového prohlížeče zadáme IP adresu routeru, která je defaultně nastavena na 192.168.0.1 a pro přístup použijeme stejné jméno i heslo „admin“. V administraci vybereme záložku Network, WAN. V této záložce musíme nastavit následující údaje, které můžete vidět v tabulce 4.1.

Typ připojení	PPPoE
Service name	musí být prázdné
Login	uai88256
Password	**********
Způsob připojení	Allways connected

Tabulka 4.1. – Nastavení VDSL routeru,
Zdroj: vlastní

Konfigurace Wi-Fi připojení

Wi-Fi připojení poběží na pásmu 2,4Ghz, protože pásmo 5Ghz pracuje na vyšší frekvenci a nedosáhne na tak velkou vzdálenost jako 2,4Ghz a má horší průchod zdí. Dále nastavíme SSID jako název firmy.

Zabezpečení

Zabezpečení bude nastaveno na WPA2/PSK se šifrováním AES. Bude použito heslo, které bude obsahovat kombinaci velkých a malých písmen, číslic a bude mít délku 10 znaků.

Nastavení LAN

V záložce LAN nastavíme IP adresu routeru na 192.168.1.1 a masku 255.255.255.0.

Nastavení DHCP

DHCP server bude nastaven následovně. Rozsah DHCP serveru bude automaticky přidělovat IP adresy dalším zařízením v rozsahu od 192.168.1.26 do 192.168.1.254 a zařízení, které mají přidělenou pevnou IP adresu mají rozsah od 192.168.1.1 do 192.168.1.11.

Router bude disponovat funkcí, která zabezpečuje selhání internetového připojení tak, že v rámci výpadku přepne na sekundární LTE připojení a jakmile bude primární připojení funkční, přepne se zpět na primární WAN. Přepnutí připojení zajišťují dvě funkce, a to Failover Mode a funkce obnovení Allow Failback.

4.3.2. Konfigurace Access Pointu

Access Point bude sloužit pro rozšíření Wi-Fi připojení do zbytku prostor. Jedná se tedy o dvoupásmové AP, které bude vysílat dvě sítě. U první sítě musí být vypnutý DHCP server, protože DHCP server je již zapnutý na hlavní routeru a tato síť slouží pouze pro rozšíření firemní sítě. Druhá síť typu Host bude nastavena tak, že hosti nebudou mít přístup do firemní sítě ale pouze do sítě internet. K nastavení přístupu hosta slouží funkce Enable Routing between Zones, pokud je tato možnost deaktivována, mají hosté přístup pouze k internetu. AP bude připojeno do zařízení typu switch a bude mít IP adresu 192.168.1.2. Pro plynulý přechod bezdrátového připojení bez ztráty spojení z routeru na AP a obráceně slouží funkce Roaming Assist.

Zabezpečení

Jako první bude změněno přihlášení do administrace routeru. Původní jméno a heslo bylo admin, admin. Takové jméno a heslo, jako defaultní, používá většina routerů a málokdo to mění a jedná se pak o velkou bezpečnostní chybu. Pro zařízení s přístupem do firemní sítě, které mají přidělené pevné IP adresy, v tomto případě počítače a laptopy, bude nastaven filtr MAC adres pro jednotlivá zařízení. Díky tomuto filtru se do firemní sítě nedostane s cizím zařízením nikdo, i když se připojí přes kabel například do ethernetové zásuvky. Názvy (SSID) routeru a Access Pointu budou změněny, bude nastaveno zabezpečení typu WPA2/PSK se šifrováním AES, kde heslo tvoří kombinaci malých/velkých písmen, speciálních znaků a číslic určité délky. Síť typu host bude mít stejné zabezpečení ale heslo bude pouze kombinace malých písmen a číslic a bude rozdávání na požádání všem zákazníkům.

4.4.Návrh koncových zařízení

V této podkapitole se budu věnovat návrhu koncových zařízení, které budou připojeny do firemní sítě. Cenové kalkulace všech nakoupených koncových zařízení naleznete v příloze 1.

4.4.1. Síťová tiskárna

Z důvodu změny IT infrastruktury, dle požadavků firmy, bude potřeba změna tiskárny, která bude umístěna v kanceláři majitele. Tiskárna bude obsahovat skener, automatický oboustranný tisk a funkci kopírky. Pro minimalizaci nákladů na neustálé dokupování barevných tonerů byla vybrána laserová černobílá tiskárna Brother DCP-L2712DW, která má minimální náklady na provoz (toner na 3000 stran). Po domluvě s majitelem bude dostačující černobílý tisk pro potřeby firmy. Síťová tiskárna řeší problém s neustále zapnutým počítačem.

4.4.2. Síťové úložiště NAS

Dle požadavků firmy bude instalováno síťové úložiště NAS pro ukládání a zálohování firemních dat. Bylo vybráno úložiště od firmy Synology, model DiskStation DS218+. Tento model je vybaven rychlým CPU o taktu 2,5Ghz, 2 GB RAM, rychlostí čtení a zápisu 113 MB/s a výkonným bezpečnostním hardwarovým šifrováním AES-NI. Do sítě bude připojen pomocí Gbit Ethernetového portu s koncovkou RJ-45. Obsahuje místo pro dva 3,5" pevné disky o maximální kapacitě 24TB.

NAS díky systému DiskStation Manager umožňuje instalaci různých aplikací včetně aplikace, která slouží pro monitorování záznamů z IP kamer v reálném čase. V neposlední řadě obsahuje funkci Cloud Station Backup, která dokáže automaticky nahrávat a synchronizovat soubory, které se ihned nahrají do úložiště, což vyřeší problém se sdílením dat. Další otázkou je bezpečnost dat, která bude popsána níže v samostatné kapitole.

Doposud bylo ukládání a sdílení dat řešeno přes sdílenou složku, přičemž musel být neustále zapnutý počítač. Síťovým úložištěm NAS se tento problém vyřešil.

Výběr pevného disku

Při výběru pevného disku do síťového úložiště je potřeba zohlednit velikost dat, které bude firma ukládat a se kterými bude pracovat. Autodílna bude pracovat ve velké míře s textovými soubory, které obsahují různé informace o objednávkách, automobilech, zákaznících, zaměstnancích, výplatách a dílech na skladě. Další data, která se budou ukládat, jsou záznamy z bezpečnostních kamer, které se budou ukládat po dobu 14 dní. Dále bude vhodné vytvořit obrazy (image) všech firemních počítačů a laptopů, z důvodu rychlého obnovení diskových oddílů při poškození systému nebo samotného počítače/laptopu. Musí se počítat i s rezervou pro případná budoucí data, určená k uložení.

Dle odhadu využití diskových kapacit byly vybrány dva pevné disky od značky Western Digital model WD Red o velikosti 2TB. Celková velikost pevných disků je tedy 4TB. Tyto disky jsou přímo určené pro dané síťové úložiště a budou zapojeny do diskového pole z důvodu spolehlivosti a bezpečnosti dat.

Celkové využití diskových kapacit můžete vidět v tabulce 4.2.

Účel	Potřebné místo celkem
Kamerové záznamy po dobu 14 dnů při rozlišení 1280 x 720 a 30FPS (2kamery)	0,85 TB
Záloha diskových oddílů (image)	0,35 TB
Firemní data	0,20 TB
Rezerva pro firemní data	0,50 TB
Celkem	**1,27 TB**

Tabulka 4.2. – Potřebné místo v GB pro jednotlivá zařízení,
Zdroj: vlastní

4.4.3. Výběr IP kamer

Při výběru bezpečnostních kamer bylo nejdůležitějšími kritérii rozlišení snímače, možnost infračerveného vidění pro záznam z kamer v noci a v poslední řadě cena. Po konzultaci byly vybrány dvě kamery, které budou natáčet prostor kanceláří a část pracovního prostoru firmy.

Technické parametry kamer můžete vidět v tabulce 4.3.

Parametr	Hodnota
Typ snímače	CMOS
Rozlišení snímače	1280 × 720 px
Komprese videa	MJPEG, H.264
Zorný úhel	139 °
Rozhraní	RJ-45, Wi-Fi
Maximální dosvit nočního vidění	15m
Funkce	Detekce pohybu

Tabulka 4.3. – Parametry IP kamer,
Zdroj: Alza, 2018 (vlastní zpracování)

4.5.Nastavení koncových zařízení

V této podkapitole bude popsáno nastavení IP kamer, síťového úložiště NAS a síťové tiskány.

4.5.1. Základní konfigurace síťového úložiště NAS

Jako první nainstalujeme pevné disky tak, že je vložíme do zařízení NAS a následně server připojíme pomocí UTP kabelu do sítě. Pak nainstalujeme Synology Disk Station pomocí aplikace Synology Disk Assistant, který se nachází na přiloženém instalačním CD. Poté zadáme adresu serveru Synology do adresního řádku webového prohlížeče, heslo necháme prázdné a jako jméno zadáme admin. Zařízení si namapuje pevné disky a vytvoří diskové pole typu RAID, Synology Hybrid RAID, bude použit typ RAID 1 z důvodu zrcadlení dat s přípustností závady jednoho disku.

Serveru přiřadíme pevnou IP adresu 192.168.1.5 s maskou 255.255.255.0 a výchozí bránou 192.168.1.0, aby komunikoval ve vnitřní síti. Nakonec bude změněno heslo k administraci serveru z bezpečnostních důvodů, jinak by se nám každý do síťového úložiště dostal přes defaultní heslo, které je veřejně známé.

Nastavení vzdáleného přístupu

Vzdálený přístup k datům na serveru bude fungovat pomocí funkce QuickConnect, která běží na systému DSM 5.0 a vyšší. Pomocí této funkce bude snadné se připojit k NAS serveru odkudkoliv ze sítě Internet bez nutnosti nastavení pravidel předávání portů nebo dalších komplikovaných síťových nastavení. Takové připojení se vytvoří na základě nastavitelného ID nebo adresy, kterou si nastavíme níže.

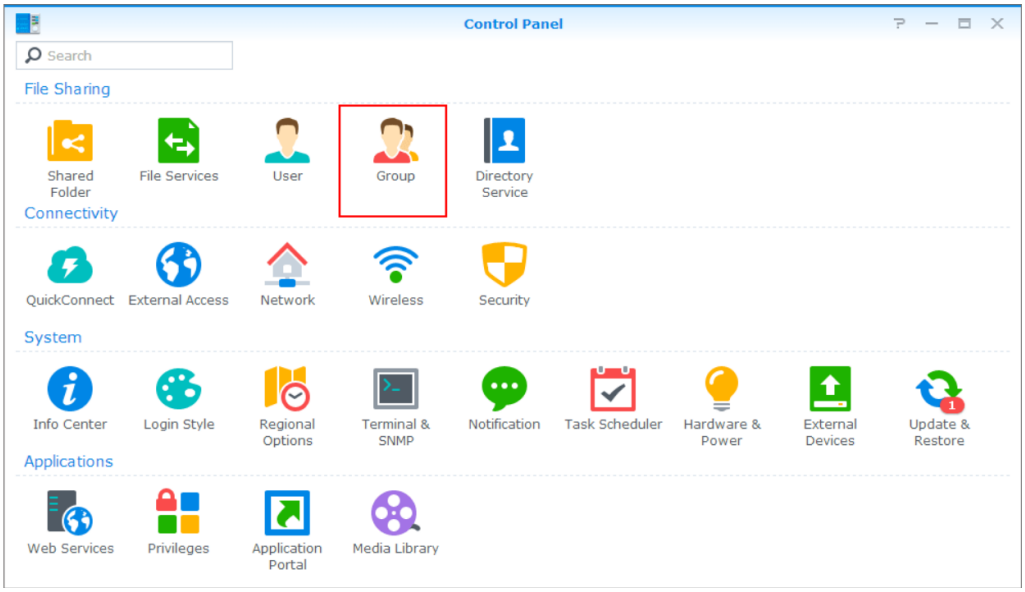
Na NAS serveru přejdeme do ovládacích panelů a povolíme funkci QuickConnect. Poté vytvoříme účet MyDS Center, kde zadáme náš e-mail, heslo a jméno. Na základě registrace nám bude přiděleno QuickConnect ID a dostaneme přístupovou adresu do NAS serveru. Adresu s ID zadáváme odkudkoliv do adresního řádku internetového prohlížeče. Tato adresa nás přesměruje na přihlašovací stránku našeho NAS serveru, kde zadáme e-mail a heslo, které jsme zadávali v registraci a dostaneme okamžitý přístup k našim datům na serveru. Příklad adresy je http://quickconnect.to/examplequickconnectID. V adrese nejsou uvedeny pravdivé údaje z důvodu zachování soukromí.

Vytvoření uživatelských skupin

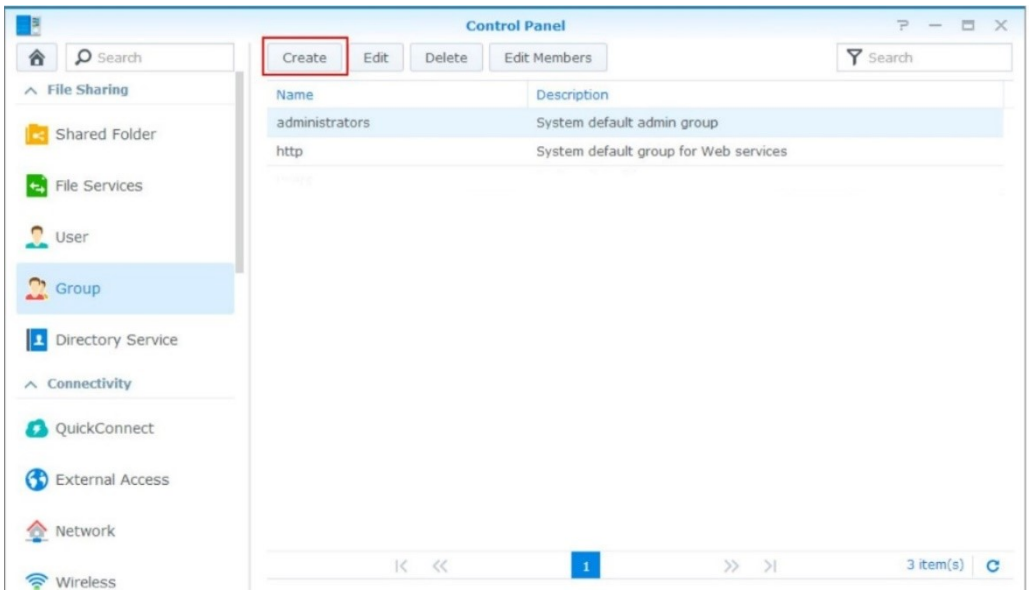
Výhodou skupin je, že každá skupina bude mít určitá oprávnění a do těchto skupin budou přiřazováni uživatelé firmy => při nahrazení nějakého zaměstnance se nebudou muset vytvářet k účtu nová oprávnění, ale nový zaměstnanec se přiřadí určité skupině.

V ovládacích panelech operačního systému NAS zvolíme kolonku Group neboli skupina. V sekci skupina klikneme na vytvořit a následně zadáme jméno a popis skupiny. Vytvořené skupiny budou: Administrator, Vedení, Zaměstnanci.

Výřezy nastavení můžete vidět na obrázku 4.4. a obrázku 4.5.



Obrázek 4.4. – Nastavení skupin 1,
Zdroj: vlastní zpracování



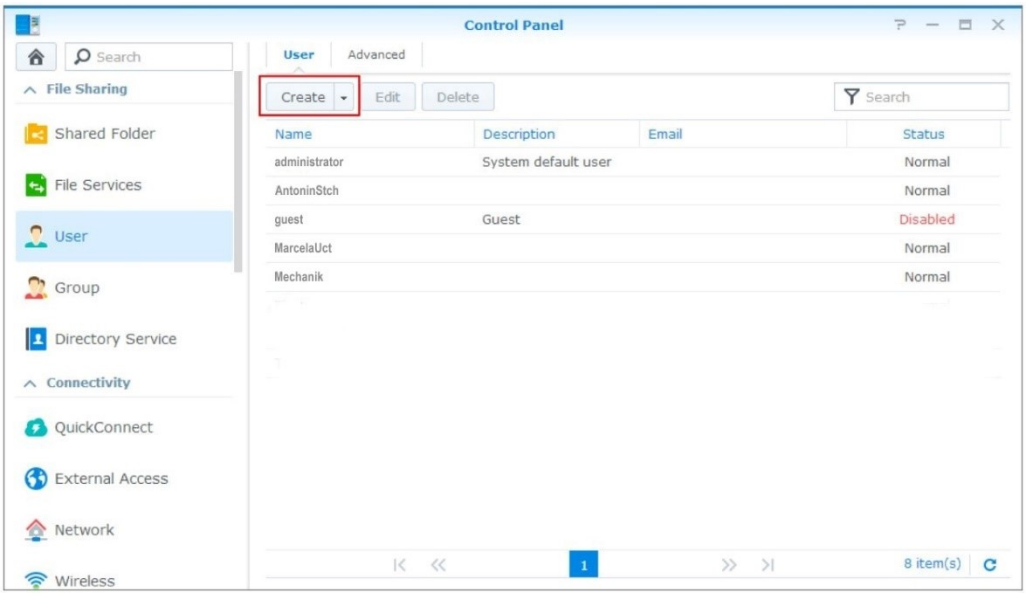
Obrázek 4.5. – Nastavení skupin 2,
Zdroj: vlastní zpracování

Vytvoření uživatelských účtů

Pro vytvoření uživatelských účtů využijeme operačního systému NAS a uplatníme tzv. Skupiny, které jsme si již vytvořili.

V ovládacích panelech operačního systému NAS zvolíme kolonku User neboli uživatel. V sekci uživatel klikneme na vytvořit a tím spustíme průvodce vytvořením uživatele. Následně zadáme jméno uživatele, popis, e-mail, heslo a můžeme uživateli zakázat měnit heslo účtu. Poté přiřadíme uživatele k již vytvořeným skupinám, která mají určitá oprávnění. Firma si nepřeje zveřejňovat informace o přiřazení uživatelů ke skupinám.

Výřez z nastavení můžete vidět na obrázku 4.6.

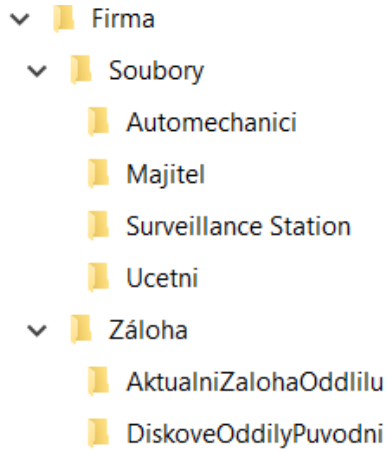


Obrázek 4.6. – Nastavení uživatelů,
Zdroj: vlastní zpracování

Vytvoření adresářové struktury

Vytvoření adresářové struktury je nezbytné pro přehled všech souborů a dat na síťovém úložišti. Pro zálohy bude vytvořena složka Záloha, kde bude uložena záloha diskových oddílů a záloha aktuálních firemní dat, jako jsou informace o automobilech, zákaznících, zaměstnancích a pohybu peněz ve firmě. Pro majitele a účetní firmy bude vytvořena složka s názvem Majitel a Ucetni. Automechanici budou mít složku s názvem Automechanici. Pro ukládání záznamů z kamer bude sloužit složka s názvem Surveillance Station, která bude popsána a nastavena níže.

Adresářovou strukturu můžete vidět na obrázku 4.7.



Obrázek 4.7. – Adresářová struktura firmy,
Zdroj: vlastní zpracování

Přístup ke sdíleným složkám

Můžeme určit, kteří uživatelé a skupiny budou přistupovat ke sdílené složce a obsahu, a tuto složku zobrazovat a upravovat. Přístupová oprávnění sdílené složky lze přizpůsobit pro jednotlivé uživatele a skupiny. Z důvodu zachování soukromí bude popsáno nastavení přístupu ke složkám bez výřezů obrazovky.

V ovládacích panelech klikneme na Shared Folder, kde můžeme vytvořit adresářovou strukturu firmy (viz obrázek 4.7.). K jednotlivým složkám pomocí tlačítka Edit nastavíme oprávnění, v našem případě budeme přiřazovat již vytvořené skupiny, které obsahují uživatele firmy.

Nastavení oprávnění ke sdíleným složkám můžete vidět v tabulce 4.4.

	Názvy sílených složek				
Název skupiny	**Majitel**	**Ucetni**	**Automechanici**	**Surveillance Station**	**Zaloha**
Administrator	R/W	R/W	R/W	R/W	R/W
Vedení	R/W	R/W	R/W	R/W	R
Zaměstnanci	No access	No access	R/W	R	R

Tabulka 4.4. – Oprávnění uživatelů ke sdíleným složkám,
Zdroj: vlastní zpracování

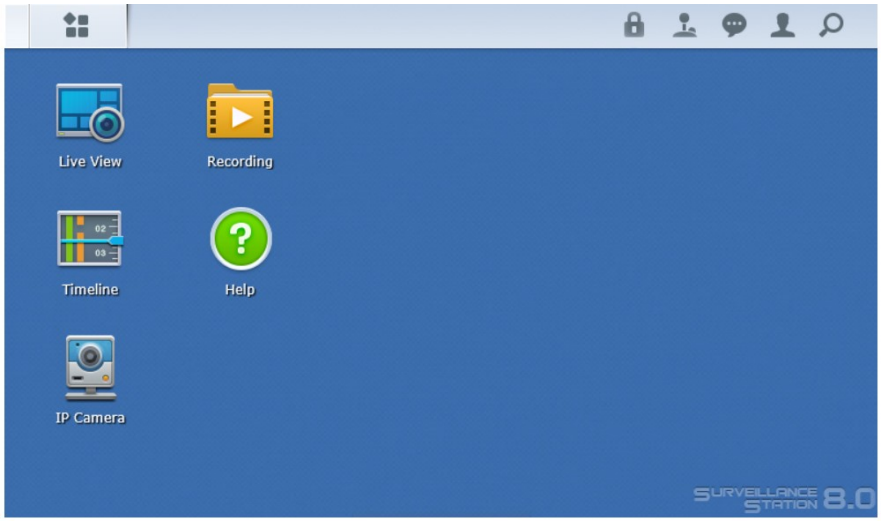
Nastavení Surveillance Station

V operačním systému NAS server můžeme instalovat různé softwarové balíky. Jedním z nich je Surveillance Station, který zajišťuje ochranu formou monitoringu pomocí IP kamer. Pomocí nabídky Přidat, přidáme IP kamery. Zadáme název kamery a přidáme pevnou IP adresu kamery, kterou jsme si určili.

Kamery budou nahrávat v rozlišení 1280 x 720 při 30 snímcích za sekundu, doba uchování záznamu bude 14 dní, bude využit kodek H.264+. Pro IP kamery bude nastaven stream, který umožní živý náhled ze systému DSM a například majitel se bude moci v reálném čase podívat, co se ve firmě děje. Rozlišení při živém náhledu bude 1280 x 720 pixelů při 15 snímcích za sekundu.

Softwarový balík si po výběru kamery nastaví sám rozlišení při nahrávání a rozlišení při živém náhledu. Nastavení ukládání záznamů po dobu 14 dní musíme nastavit u každé kamery zvlášť. U výběru kamer povolíme dočasný záznam, kde nastavíme plán nahrávání a dobu uchování záznamu. Firma si nepřeje zveřejnit výřez nastavení z důvodu citlivých informací o kameře.

V náhledu programu na obrázku 4.7. můžeme vidět jednoduché uživatelské rozhraní. Uživatel může jednoduše přejít do živého náhledu (Live View) nebo do Recording, kde se nachází dočasné záznamy z kamer.

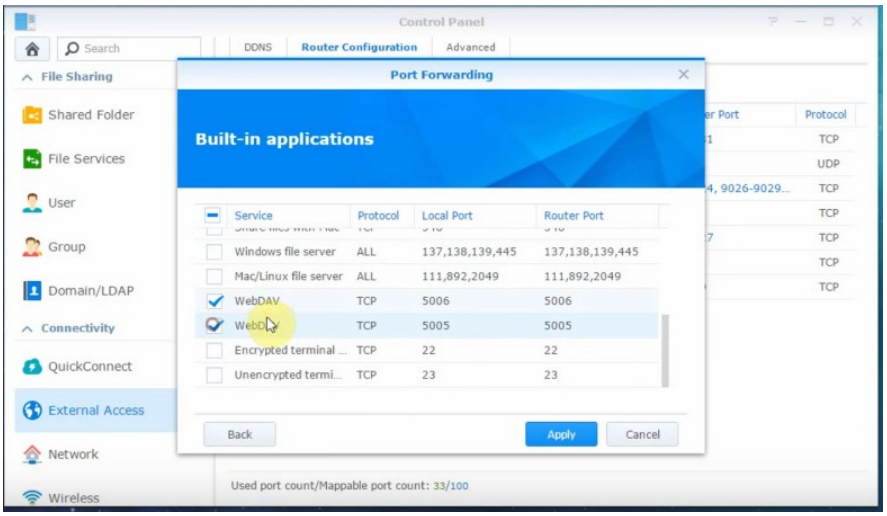


Obrázek 4.7. – Uživatelské rozhraní Surveillance Station,
Zdroj: vlastní zpracování

Nastavení přístupu z vnitřní sítě

Abychom mohli k NAS server přistupovat z každého počítače připojeného do firemní sítě, musíme nastavit port, na kterém bude server komunikovat ve vnitřní síti.

Nastavení portů můžete vidět na obrázku 4.8.



Obrázek 4.8. – Nastavení portů pro namapování NAS server,
Zdroj: vlastní zpracování

Poté na každém počítači ve firemní síti pomocí funkce namapování disku, bude přidán zástupce NAS serveru, který bude vystupovat jako nový disk, podobně jako např. (C:).

4.5.2. Nastavení síťové Tiskárny

Aby nám tiskárna fungovala v rámci sítě, musíme ji správě nastavit. Jako první bude tiskárně přidělena pevná IP adresa, a to 192.168.1.4 s maskou 255.255.255.0 a výchozí bránou 192.168.1.0. Díky tomuto nastavení, bude možné tisknou z tiskárny v rámci firemní sítě.

Princip sdílené síťové tiskárny bude fungovat tak, že z kteréhokoliv počítače připojeného do firemní sítě bude možné odeslat dokument do tisku, který se vytiskne v kanceláři majitele. Skenování bude probíhat pouze z počítače v kanceláři majitele pomocí softwaru tiskárny. Takové nastavení je pro firmu dostačující a není potřeba žádné sdílené složky pro ukládání skenovaných dokumentů.

4.5.3. Nastavení IP kamer

Z důvodu síťového fungování IP kamer nastavíme první kameře IP adresu 192.168.1.9 a druhé kameře přidělíme IP adresu 192.168.1.10, výchozí brána u obou kamer bude 192.168.1.0. Přístup ke kamerám byl již nastaven v rámci konfigurace síťového úložiště NAS, konkrétně nastavení přístupů do složky Surveillance Station.

4.5.4 Nastavení počítače a notebooků

Nakonec budou nastaveny notebook a stolní počítač. Stolnímu počítači v kanceláři majitele bude přiřazena pevná IP adresa 192.168.1.3. Notebooky budou mít IP adresy 192.168.1.6 a 192.168.1.7. Síťová maska bude stejná 255.255.255.0 s výchozí bránou 192.168.1.0. Pro přístup z vnitřní sítě byl na každý počítač ve firmě namapován NAS server v podobě disku, (viz Konfigurace NAS – nastavení přístupu z vnitřní sítě).

Účetnictví a stav skladu bude nadále řešen z počítače účetní, na který byl z instalačního CD nainstalován software Pohoda.

Zařízení, které se budou připojovat k síti host, budou mít přiděleny IP adresy z DHCP serveru.

5 Výsledné zhodnocení navrženého IT řešení

V této kapitole bude shrnuto finanční hledisko celého projektu a celé IT řešení bude zhodnoceno i z hlediska funkčního a implementačního. Nové IT řešení bude navrhnuto majiteli firmy, který rozhodne o následné realizaci projektu.

5.1.Finanční hledisko návrhu

V této podkapitole bude shrnuto finanční hledisko navrženého hardwaru, tj. aktivních a pasivních prvků počítačové sítě i koncových zařízení.

Finanční přehled můžete vidět v tabulce 5.1.

Zařízení	Položka	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
VDSL router	ASUS DSL-AC55U	1	2644 Kč	2644 Kč
Switch	TP-LINK TL-SG108	2	826 Kč	1652 Kč
Zásuvky	Datacom RJ-45 CAT6 STP, 2x RJ45	2	164 Kč	328 Kč
Access Point	TP-LINK RE305 AC1200 Dual Band	1	1074 Kč	1074 Kč
Síťová tiskárna	Brother DCP-L2712DW	1	3798Kč	3798 Kč
NAS server	Synology DiskStation DS218+	1	7678Kč	7678 Kč
Pevné disky NAS	WD Red 2TB	2	1644Kč	3288 Kč
IP kamery	Edimax IC-9110W	2	2802Kč	5604 Kč
Celkové vypořádání		**12**		**26066 Kč**

Tabulka 5.1. – Celkový finanční přehled hardwarových prvků a koncových zařízení, Zdroj: vlastní

Finanční hledisko projektu bylo omezeno rozpočtem v rozmezí 20 000 – 40 000 Kč. Majiteli záleželo jen na dodržení rozpočtu a nijak nezasahoval do vybíraného hardwaru. Celková cena hardwaru činí 26 066 Kč, tudíž byl rozpočet splněn. Firma rozhodla, že rozpočet je adekvátní přínosu a nic nebrání realizaci implementaci navrženého IT řešení.

5.2.Implementace IT řešení

Firma se po přijetí finanční analýzy rozhodla implementovat navržené IT řešení. Ze zkušeností pracovního nasazení i z jiných autoservisů bylo zjištěno, že nejméně zákazníků je v měsíci leden, proto implementace projektu proběhla v lednu 2018.

5.3.Funkční hledisko návrhu

Implementace IT řešení byla realizována v lednu roku 2018. Nově navržené IT řešení již funguje necelé 4 měsíce bez problémů a je pro firmu velkým přínosem. Ve firmě došlo ke zrychlení některých podnikových procesů, jako sdílení dat, účetnictví a vedení skladové evidence. Nový poskytovatel internetu je natolik spolehlivý, že doposud nedošlo k žádnému výpadku sítě ani většímu zpomalení rychlosti internetu. Firma doposud nevyzkoušela rezervní internetové připojení s technologií LTE, které však bylo testováno a funguje bezchybně. Kromě zvýšené bezpečnosti dat bylo velkým přínosem i síťové úložiště a vzdálený přístup k datům, což ocenili hlavně automechanici mimo provozovnu u zákazníků.

Firma je celkově schopna přijmout a obsloužit větší počet zákazníků, zaměstnanci mají okamžitý přístup k firemním datům a zákazníci si mohou zpříjemnit čekání surfováním na internetu bez ohrožení bezpečnosti firemních dat.

6 Závěr

Tato práce byla zaměřena na návrh nového IT řešení pro firmu zabývající se opravou osobních automobilů.

V první řadě bylo nutné provést analýzu aktuálního IT řešení ve firmě včetně jejího interního prostředí. Po výsledcích, které vyplývaly z analýzy současného stavu, byl vypracován návrh nového IT řešení dle požadavků firmy. Byl navrhnut vhodný hardware včetně koncových zařízení a poté bylo provedeno jejich nastavení. Navržené řešení internetového poskytovatele bylo testováno na stabilitu, rychlost připojení a výsledky byly pro firmu velmi přínosné.

Autoservis se rozhodl IT řešení implementovat v lednu 2018 a je pravděpodobné, že s novou IT infrastrukturou bude fungovat ještě řadu let. Nové IT řešení poskytlo firmě lepší bezpečnost a sdílení dat, automatizaci některých podnikových procesů, stabilnější internetové připojení, vzdálený přístup k datům a pravidelné zálohy citlivých firemních dat. Celkově se zrychlí pohyb ve skladu, účetnictví a zjišťovaní důležitých informací z kteréhokoliv firemního počítače. Díky těmto změnám je firma schopna obsloužit více zákazníků už jen kvůli rozšířeným prostorům, které jsou teď plně zasíťované.

Pro případné budoucí rozšíření počítačové sítě jsou k dispozici volné porty a IP adresy pro připojení dalších zařízení. Firma plánuje v budoucnu rozšířit svůj prostor, kdy tyto rezervy pro další zařízení určitě ocení.

Na základě uvedených údajů, byl cíl této bakalářské práce, který zahrnoval návrh a optimalizaci IT řešení pro autodílnu splněn.

Seznam použité literatury

Odborná literatura

BAGAD, V. S. a I. A. DHOTRE. Computer Networks. India: Technical Publications Pune, 2009. ISBN 9788184316179.

BROŽOVÁ, Helena, Milan HOUŠKA a Tomáš ŠUBRT. Modely pro vícekriteriální rozhodování. Praha: Credit, 2003. ISBN 80-213-1019-7.

BURIAN, Pavel. Internet inteligentních aktivit. Praha: Grada, 2014. Průvodce (Grada). ISBN 978-80-247-5137-5.

CAFOUREK, Bohdan. Windows 7: kompletní příručka. Praha: Grada, 2010. Profesional. ISBN 978-80-247-3209-1.

DEAN, Tamara. CompTIA Network+ 2009 in depth. Boston, Mass.: Course Technology/Cengage Learning, c2009. ISBN 1598638785.

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

CHROMÝ, Jan. Informační a komunikační technologie pro hotelnictví a cestovní ruch. Praha: Vysoká škola hotelová v Praze 8, 2008. ISBN 978-80-86578-76-7.

JURÁŠKOVÁ, Olga a Pavel HORŇÁK. Velký slovník marketingových komunikací. Praha: Grada, 2012. ISBN 978-80-247-4354-7.

KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání. Brno: Albatros Media, 2012. ISBN 970-80-251-2236-5.

KLEMENT, Milan. Technologie bezdrátových sítí – základní principy a standardy. Olomouc: Univerzita Palackého, 2017. ISBN 978-80-244-5156-5.

PROCHÁZKA, David. První kroky s internetem. 3., aktualiz. vyd. Praha: Grada, 2010. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.

SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. Brno: Computer Press, 2012. ISBN 978-80-251-3718-5.
SHIMONSKI, Robert., Richard T. STEINER a Sean M. SHEEDY. Network cabling illuminated. Sudbury, Mass: Jones and Bartlett, c2006. ISBN 0763733938.

SLAVÍK, Petr. Windows 8 - kompletní příručka. Praha: Grada Publishing, 2013. ISBN 978-80-247-4340-0.

SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

ŠILHAVÝ, Radek, Petr ŠILHAVÝ, Zdenka PROKOPOVÁ, Pavel POKORNÝ, Martin SYSEL, Miroslav MATÝSEK, Karel VLČEK a Libuše SVOBDOVÁ. Vybrané aspekty návrhu webových informačních systémů. Vsetín: Scientific Press, 2013. ISBN 978-80-904741-3-0.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada, 2009. Profesionál. ISBN 978-80-247-2098-2.

ZELINKA, Tomáš a Miroslav SVÍTEK. Telekomunikační řešení pro informační systémy síťových odvětví. Praha: Grada, 2009. Průvodce (Grada). ISBN 978-80-247-3232-9.

Elektronické dokumenty a ostatní

10 gigabit Ethernet (10 GbE). Tech Target: Search Networking [online]. 2013, 2013 [cit. 2018-04-18]. Dostupné z: https://searchnetworking.techtarget.com/definition/10-Gigabit-Ethernet

DSL.CZ, Redakce. 2,5Gb/s a 5Gb/s Ethernet. DSL [online]. 2016, 2016 [cit. 2018-04-18]. Dostupné z: http://www.dsl.cz/clanky/byl-schvalen-standard-pro-2-5gbs-a-5gbs-ethernet

Typy RAID. In: Digitální Domácnost [online]. SiteWizard, 2014 [cit. 2018-05-04]. Dostupné z: http://www.digitalnidomacnost.cz/jaky-raid-nasadit-v-nas/

Wi-Fi Data Rates, Channels and Capacity: IEEE 802.11ac and 802.11ax. Home toys [online]. Qorvo company, 2018, 2018 [cit. 2018-04-19]. Dostupné z: https://www.hometoys.com/article/2018/01/wi-fi-data-rates-channels-and-capacity/37787

Seznam zkratek

AES	Advanced Encryption Standard
CAN	Campus Area Network
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
CLI	Command Line Interface
CSMA/CD	Carrier Senes Multiplne Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Disk Operating System
DPH	Daň z přidané hodnoty
DSM	DiskStation Manager
EDGE	Enhanced Data rates for GSM Evolution
FTP	File Transfer Protocol
EMI	Electromagnetic Interference
Gb/s	Rychlost v Gbitech za sekundu
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HDD	Hard Disk Drive
HSDPA	High-Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IPI	Internet Protocol
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
ISP	Internet Service Provider

LAN	Local Area Network
LTE	Long Term Evolution
MAN	Metropolitan Area Network
Mb/s	Rychlost v Mbitech za sekundu
Mhz	Megahertz
NAS	Network Attached Storage
PPPOE	Point-to-Point Protocol over Ethernet
QOS	Quality of Service
RAID	Redundant Array of Independent Disks
SSID	Service Set Identifier
SNMP	Simple Network Management Protocol
STP	Shielded Twisted Pair
TCP	Transmition Control Protocol
TKIP	Temporal Key Integrity Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDSL	Very high bit rate digital subscriber line
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WI-FI	Wireless-Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Acces

Příloha 3: Prohlášení o využití výsledků diplomové (bakalářské) práce

Prohlašuji, že

- jsem byl(a) seznámen(a) s tím, že na mou diplomovou (bakalářskou) práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová (bakalářská) práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 9. 5. 2018

.....

Jaroslav Beňa